



CABLE

SATELLITE

TELECOM

TERRESTRIAL

TWG870 - Wireless Voice Gateway

User manual

THOMSON

CAUTION

Disconnect power before servicing.

This device is intended for indoor operation only.

Telephone jacks Line 1 and Line 2 must not be connected to outside wiring.

CAUTION

To ensure reliable operation and to prevent overheating, provide adequate ventilation for this modem and keep it away from heat sources. Do not locate near heat registers or other heat-producing equipment. Provide for free air flow around the Wireless Voice Gateway and its power supply.



This symbol means that your inoperative electronic appliance must be collected separately and not mixed with the household waste. The European Union has implemented a specific collection and recycling system for which producers are responsible.

This appliance has been designed and manufactured with high quality materials and components that can be recycled and reused. Electrical and electronic appliances are liable to contain parts that are necessary in order for the system to work properly but which can become a health and environmental hazard if they are not handled or disposed of in the proper way. Consequently, please do not throw out your inoperative appliance with the household waste.

If you are the owner of the appliance, you must deposit it at the appropriate local collection point or leave it with the vendor when buying a new appliance.

- If you are a professional user, please follow your supplier's instructions.

- If the appliance is rented to you or left in your care, please contact your service provider.

Help us to protect the environment in which we live!

NORTH AMERICAN CABLE INSTALLER:

This reminder is provided to call your attention to Article 820-40 of the National Electrical Code (Section 54 of the Canadian Electrical Code, Part 1) which provides guidelines for proper grounding and, in particular, specifies that the cable ground shall be connected to the grounding system of the building as close to the point of cable entry as practical.

Euro-PacketCable and Euro-DOCSIS compliant

This product was designed according to Euro-PacketCable Specifications, Euro-DOCSIS Specifications and Data over Cable Service Interface Specifications.

Operating Information

Operating Temperature: 0° - 40° C (32° - 104° F)

Storage Temperature: -30° to 65° C (-22° - 149° F)

If you purchased this product at a retail outlet, please read the following:

Product Information

Keep your sales receipt to obtain warranty parts and service and for proof of purchase. Attach it here and record the serial and model numbers in case you need them. The numbers are located on the back of the product.

Model No. _____ Serial No _____

Purchase Date: _____ Dealer/Address/Phone: _____

Table of Contents

Chapter 1: Connections and Setup	5
Turning on the Wireless Voice Gateway	5
Introduction.....	5
Wireless Voice Gateway Features.....	5
What's on the CD-ROM	7
Computer Requirements	8
Wall Mounting.....	9
Wireless Voice Gateway Overview	10
Front Panel	10
rear Panel	13
Relationship among the Devices	14
What the Modem Does.....	14
What the Modem Needs to Do Its Job	15
Contact Your Local Cable Company	16
Connecting the Wireless Voice Gateway to a Single Computer.....	17
Attaching the Cable TV Wire to the Wireless Voice Gateway	17
Important Connection Information	18
Ethernet Connection to a Computer	19
Connecting More Than A Computer to the Wireless Voice Gateway	20
Telephone or Fax Connection.....	21
Chapter 2: WEB Configuration.....	22
Accessing the Web Configuration.....	22
Outline of Web Manager.....	23
Warning message to change the password	24
Gateway – Status Web Page Group	25

Table of Contents

1. Software	25
2. Connection	26
3. Password.....	27
4. Diagnostics.....	29
5. Event Log.....	30
6. Initial Scan	31
7. Backup/Restore.....	32
Gateway – Network Web Page Group.....	33
1. LAN	33
2. WAN.....	34
3. Computers	35
4. DDNS - Dynamic DNS service	36
5. Time server.....	37
6. FTP Diagnostics.....	38
7. Portbase PassThrough.....	39
Gateway – Advanced Web Page Group	40
1. Options.....	40
2. IP Filtering	42
3. MAC Filtering	43
4. Port Filtering.....	44
5. Forwarding	45
6. Port Triggers	46
7. DMZ Host	47
8. RIP (Routing Information Protocol) Setup.....	48
Gateway – Firewall Web Page Group	49

Table of Contents

1. Web Content Filtering.....	49
2. TOD Filtering.....	50
3. Local Log and Remote Log.....	51
Gateway – Parental Control Web Page Group.....	52
1. Basic.....	52
Gateway – Wireless Web Page Group.....	53
1. 802.11b/g/n Radio	54
2. 802.11b/g/n Primary Network.....	56
3. Guest Network.....	65
4. Access Control.....	67
5. 802.11Advanced	68
6. Bridging.....	70
7. 802.11e QoS (WMM) Settings.....	71
VoIP – Basic Web Page Group.....	72
1. Basic LAN	72
2. Hardware Info	73
3. Event Log.....	74
4. CM State.....	76
Chapter 3: Networking	77
Communications	77
Type of Communication	77
Cable Modem (CM) Section.....	78
Networking Section.....	78
Three Networking Modes	79
Cable Modem (CM) Mode	79

Table of Contents

Residential Gateway (RG) Mode	81
Chapter 4: Additional Information	83
Frequently Asked Questions	83
General Troubleshooting	85
Service Information	86
Glossary	87

Chapter 1: Connections and Setup

Chapter 1: Connections and Setup

Turning on the Wireless Voice Gateway

If there is no lighted LEDs on the front panel, check the power on/off switch position on the back panel of Wireless Gateway: it must be "ON" = "1".

After installing the Wireless Voice Gateway and turn it on for the first time (and each time the modem is reconnected to the power), it goes through several steps before it can be used. Each of these steps is represented by a different pattern of flashing lights on the front of the modem.

Note: All indicators flash once before the initialization sequence.

If both DS and US LEDs are flashing, it means the Wireless Voice Gateway is automatically updating its system software. Please wait for the lights to stop flashing. Do not remove the power supply, switch off (on/off switch) or reset the Wireless Voice Gateway during this process.

Introduction

Wireless Voice Gateway Features

- High Speed Data Service Solution
- EuroDOCSIS 3.0 cable modem, dual-mode (DOCSIS / EuroDOCSIS)
- Giga Ethernet router with 4x Standard RJ-45 connectors for 10/100/1000Mbps. Auto-negotiation and MDIS functions
- Wi-Fi 11n wireless connection
- Wireless security: multiple SSID and WPS solution
- Two RJ-11 Foreign Exchange Station (FXS) ports for phone and fax connections
- Support simultaneous voice and data communications
- Two simultaneous voice conversations in the different FXS ports with different CODEC: PCM A-law, PCM-law, G.723.1, G.729, G.729a, G.729e, G.728, G.726, BV16 and BV32
- Echo Cancellation
- Voice Active Detection (VAD)
- DTMF detection and generation
- Comfort Noise Generation (CNG)
- Support V.90 fax and modem services
- RSA and 56 bit DES data encryption security

Chapter 1: Connections and Setup

- SNMP network management support
- IPv4 and IPv6
- Advanced security features
- Support Web pages and private DHCP server for status monitoring
- Clear LED display
- Plug and Play

Chapter 1: Connections and Setup

What's on the CD-ROM

Insert the Wireless Voice Gateway CD-ROM into your CD-ROM drive to view troubleshooting tips, the internal diagnostics, and other valuable information.

CD-ROM Contents:

- Electronic copy of this user's guide in additional languages (PDF format)
- Adobe Acrobat Reader — application you can load to read PDF format, if you don't have it loaded already
- Links to Thomson web site

EuroDOCSIS and EuroPacketCable are trademarks of Cable Television Laboratories, Inc.

Chapter 1: Connections and Setup

Computer Requirements

For the best possible performance from your Wireless Voice Gateway, your personal computer must meet the following minimum system requirements (note that the minimum requirements may vary by cable companies):

	IBM PC COMPATIBLE	MACINTOSH**
CPU	Pentium preferred	PowerPC or higher
System RAM	16MB (32MB preferred)	24MB (32MB preferred)
Operating System	Windows* NT / 2000 / Me / XP / Vista / Windows 7, Linux	Mac OS** 7.6.1 or higher
Sound Card	Required for audio on CD-ROM	N/A
Video	VGA or better (SVGA preferred)	VGA or better (SVGA built-in preferred)
CD-ROM Drive	Required	Required
Ethernet	10BaseT , 100BaseT or 1000BaseT 10BaseT , 100BaseT or 1000BaseT An Ethernet card makes it possible for your computer to pass data to and from the internet. You must have an Ethernet card and software drivers installed in your computer. You will also need a standard Ethernet cable to connect the Ethernet card to your Wireless Voice Gateway.	
Software	<ul style="list-style-type: none">• A TCP/IP network protocol for each machine• Microsoft Internet Explorer 4.0 or later or Netscape Navigator 4.0 or later.	

* Windows is a trademark of Microsoft Corporation.

** Macintosh and the Mac OS are trademarks of Apple Computer, Inc.

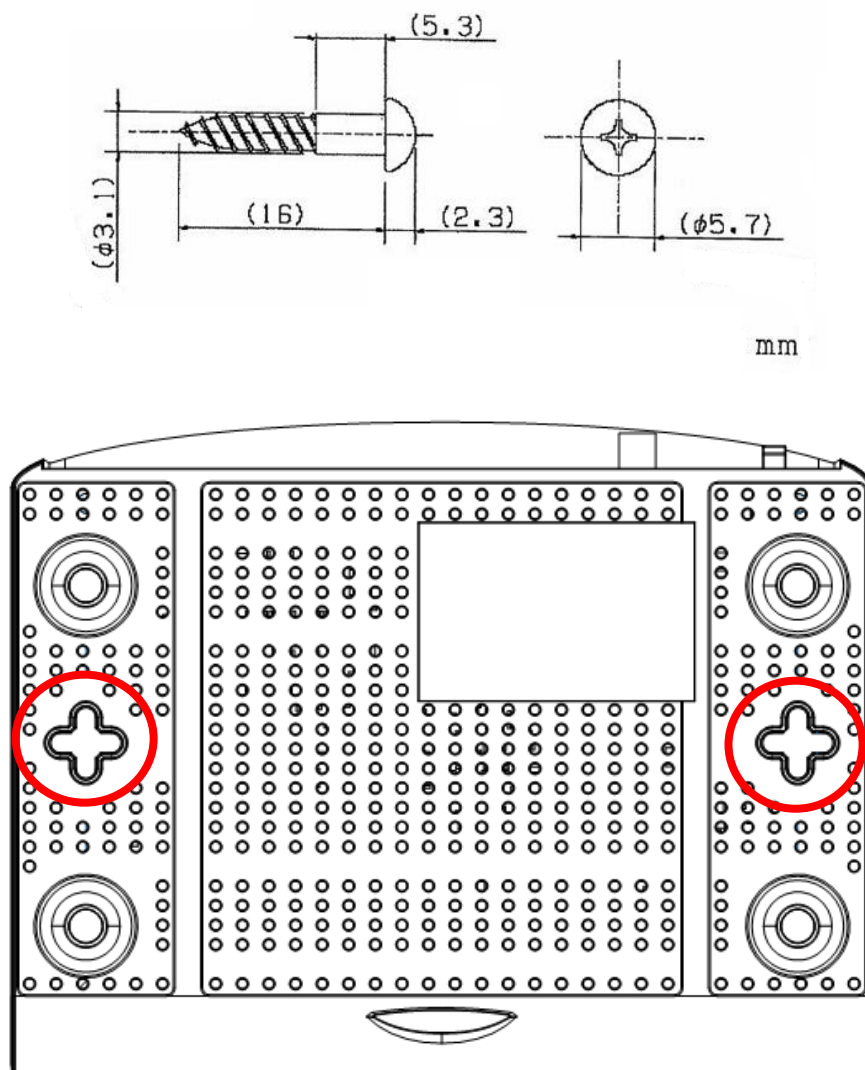
Chapter 1: Connections and Setup

Wall Mounting

This article will show the user through the process of wall-mounting the Wireless Gateway

The Adapter has two wall-mount slots on its back panel.

Two screws are needed to mount the Adapter.



To do this:

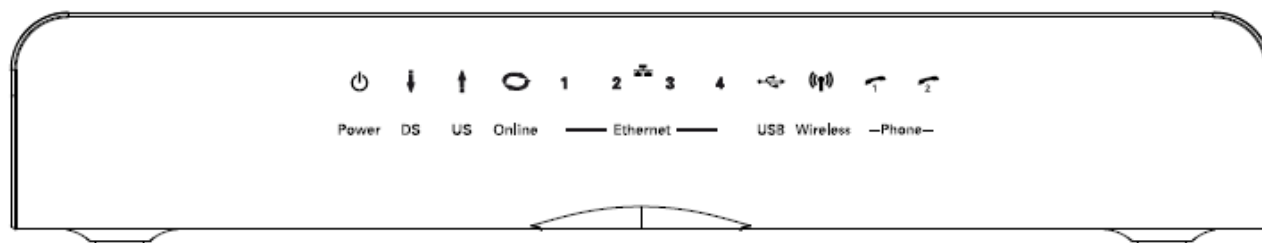
1. Ensure that the wall you use is smooth, flat, dry and sturdy and use the 2 screw holes which are 101.6 mm (4 inches) apart from each other.
2. Fix the screws into wall, leaving their heads 3 mm (0.12 inch) clear of the wall surface.
3. Remove any connections to the unit and locate it over the screw heads. When in line, gently push the unit on to the wall and move it downwards to secure.

Chapter 1: Connections and Setup

Wireless Voice Gateway Overview

Front Panel

The following illustration shows the front panel of the Wireless Voice Gateway:



The LEDs on the front panel are described in the table below (from left to right):

	Power	Internet			Ethernet				USB	Wireless	Tel 1	Tel 2	Description
		DS	US	Online	1	2	3	4					
Boot-up Operation	ON	ON	ON	ON	ON	ON	ON	ON	ON	X	ON	ON	Power on 0.25 sec
	ON	0.25 second											
	ON	FLASH	FLASH	FLASH	X	X	X	X	X	X	X	X	From power ON to system initialization complete
	ON	ON	ON	ON	X	X	X	X	X	X	X	X	Following system initialization complete to (before) DS scanning
1 second													
DOCSIS Start-up Operation	ON	FLASH	OFF	OFF	X	X	X	X	X	X	X	X	During DS scanning and acquiring SYNC
	ON	ON	FLASH	OFF	X	X	X	X	X	X	X	X	From SYNC completed, receiving UCD to ranging completed
	ON	ON	ON	FLASH	X	X	X	X	X	X	X	X	During DHCP, configuration file download, registration, and Baseline Privacy initialization: DHCP status: 1 second ON and 1 second OFF, TFTP status: 0.25 second ON and 0.25 second OFF
	ON	ON	ON	ON	X	X	X	X	X	X	X	X	Operational (NACO=ON)
	ON	FLASH	FLASH	OFF	X	X	X	X	X	X	X	X	Operational (NACO=OFF)

Chapter 1: Connections and Setup

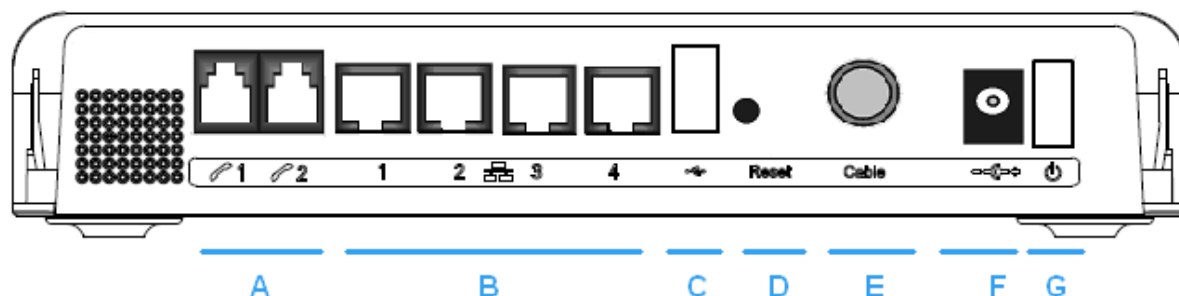
	Power	Internet			Ethernet				USB	Wireless	Tel 1	Tel 2	Description
		DS	US	Online	1	2	3	4					
Channel Bonding Operation	FLASH	FLASH	FLASH	FLASH	X	X	X	X	X	X	X	X	Wait registration with all DS and all US – Lights Flash sequentially from the right to left Minimum duration 3 seconds
	X	X	X	X	X	X	X	X	X	X	X	X	From 1 to 4 DS, from 1 to 4 LEDs are ON. From 5 to 8 DS, From 1 to 4 LEDs are flashing Duration 3 seconds
	OFF	X	X	OFF	X	X	X	X	X	X	X	X	From 1 to 2 US, from 2 to 3 LEDs are ON, from 3 to 4 US, from 2 to 3LEDs are flashing. Duration 3 seconds
	FLASH	FLASH	FLASH	FLASH	X	X	X	X	X	X	X	X	Wait registration with all DS and all US – Lights Flash sequentially from the left to right Minimum duration 3 seconds
MTA initialization	ON	ON	ON	ON	X	X	X	X	X	X	FLASH	OFF	MTA DHCP
	ON	ON	ON	ON	X	X	X	X	X	X	OFF	FLASH	MTA SNMP/TFTP
	ON	ON	ON	ON	X	X	X	X	X	X	FLASH	FLASH	RSIP
CPE Operation	ON	X	X	X	OFF ON	OFF ON	OFF ON	OFF ON	X	X	X	X	No Ethernet Link Ethernet Link TX/RX Ethernet Traffic
	ON	X	X	X	X	X	X	X	OFF ON FLASH	X	X	X	No USB Link USB Link TX/RX USB Traffic
	ON	X	X	X	X	X	X	X	X	OFF ON FLASH	X	X	No Wireless Link Wireless Link TX/RX Wireless Traffic
MTA Operation	ON	<CM Normal Operation>									ON	ON	Both Lines On-Hook
	ON										FLASH	ON	Tel1 Off-hook, Tel2 On-hook
	ON										ON	FLASH	Tel1 On-hook, Tel2 Off-hook
	ON										FLASH	FLASH	Both Lines Off-Hook

Chapter 1: Connections and Setup

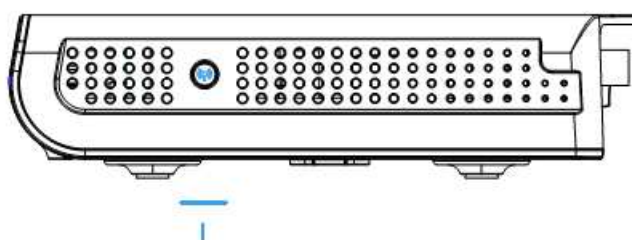
SW Download Operation	ON	FLASH	FLASH	ON	X	X	X	X	X	X	X	X	Software Download (including FLASHING of Memory)
-----------------------------	----	-------	-------	----	---	---	---	---	---	---	---	---	---

Chapter 1: Connections and Setup

rear Panel



- | | | |
|---|-------------------|--|
| A | TEL1 & TEL2 | 2x Telephony RJ-11 connectors |
| B | ETHERNET 1 2 3 4: | 4x Ethernet 10/100/1000 Mbps RJ-45 connectors |
| C | USB Host: | 1x USB 2.0 Connector |
| D | Reset: | 1x Reset or reset to factory default this Wireless Voice Gateway |
| E | CABLE: | 1x F-Connector for the coax cable |
| F | 12VDC : | 1x Power connector to connect the AC power supply |
| G | Power switch: | 1x switch to power on/off this Wireless Voice Gateway |

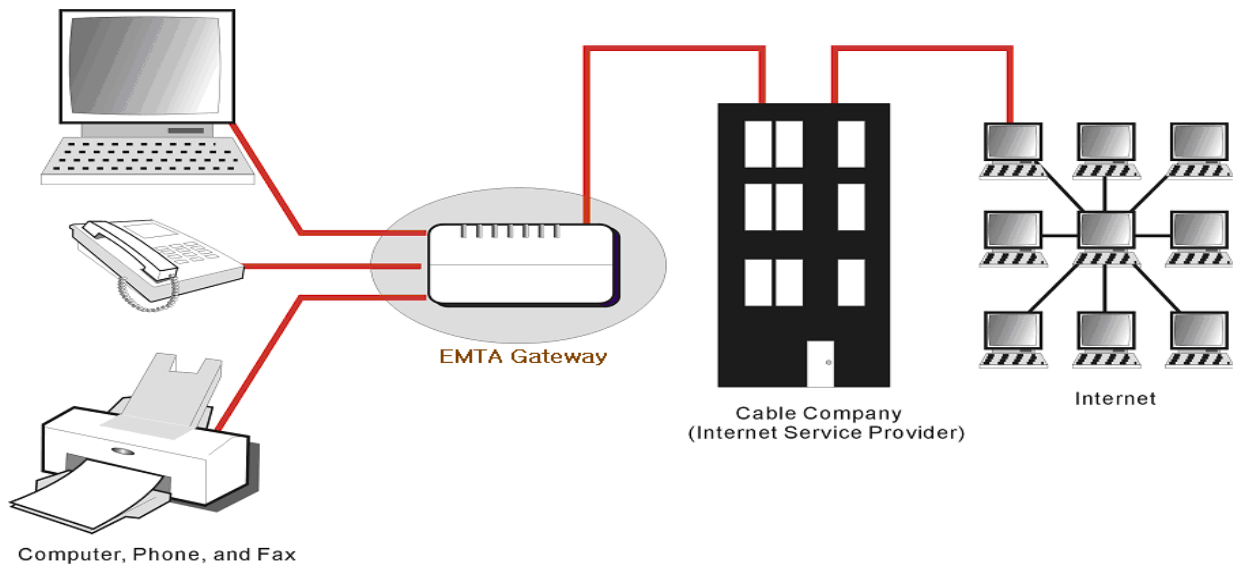


- | | | |
|---|---------------------------|--|
| I | WPS & WiFi on/off button: | 1x button with two features:
to activate/disable the WiFi, to execute a WPS association |
|---|---------------------------|--|

Chapter 1: Connections and Setup

Relationship among the Devices

This illustration shows a cable company that offers Euro-DOCSIS- and Euro-PacketCable-compliant voice/data services.



What the Modem Does

The Wireless Voice Gateway provides high-speed Internet access as well as cost-effective, toll-quality telephone voice and fax/modem services over residential, commercial, and education subscribers on public and private networks via an existing CATV infrastructure. It can inter-operate with the Euro-PacketCable compliant head-end equipment and provide the IP-based voice communications. The IP traffic can transfer between the Wireless Voice Gateway and Euro-DOCSIS compliant head-end equipment. The data security secures upstream and downstream communications.

Chapter 1: Connections and Setup

What the Modem Needs to Do Its Job

- **The Right Cable Company:** Make sure your local cable company provides data services that use cable TV industry-standard Euro-DOCSIS compliant and Euro-PacketCable compliant technology.
- **The Internet/Telephony Service Provider (ISP/TSP):** Your cable company provides you access to an Internet Service Provider (ISP) and Telephony Service Provider (TSP). The ISP is your gateway to the Internet and provides you with a pipeline to access Internet content on the World Wide Web (WWW). The TSP provides you with telephony access to other modems or other telephony services over the Public Switched Telephone Network (PSTN).

Check with your cable company to make sure you have everything you need to begin; they'll know if you need to install special software or re-configure your computer to make your cable internet service work for you.

Chapter 1: Connections and Setup

Contact Your Local Cable Company

You will need to contact your cable company to establish an Internet account before you can use your gateway. You should have the following information ready (which you will find on the sticker on the gateway):

- The serial number
- The model number
- The Cable Modem (CM) Media Access Control (MAC) address
- The Terminal Adapter (EMTA) MAC address
- Security information: Service Set Identifier (SSID), Encryption key / passphrase (WPA2-PSK by default), channel number. Default values are indicated underneath the modem on the sticker.

Please verify the following with the cable company

- The cable service to your home supports Euro-DOCSIS compliant two-way modem access.
- Your internet account has been set up. (The Media Terminal Adapter will provide data service if the cable account is set up but no telephony service is available.)
- You have a cable outlet near your PC and it is ready for Cable Modem service.

Note: It is important to supply power to the modem at all times. Keeping your modem plugged in will keep it connected to the Internet. This means that it will always be ready whenever you need.

Important Information

Your cable company should always be consulted before installing a new cable outlet. Do not attempt any rewiring without contacting your cable company first.

Please verify the following on the Wireless Voice Gateway

The on/off button on the rear panel must be in the ON mode = on “1”

Chapter 1: Connections and Setup

Connecting the Wireless Voice Gateway to a Single Computer

This section of the manual explains how to connect your Wireless Voice Gateway to Ethernet port on your computer and install the necessary software. Please refer to Figure 1 to help you connect your Digital Cable Modem for the best possible connection.

Attaching the Cable TV Wire to the Wireless Voice Gateway

1. Locate the Cable TV wire. You may find it one of three ways:
 - a. Connected directly to a TV, a Cable TV converter box, or VCR. The line will be connected to the jack, which should be labeled either IN, CABLE IN, CATV, CATV IN, etc.
 - b. Connected to a wall-mounted cable outlet.
 - c. Coming out from under a baseboard heater or other location. See Figure 1 for the wiring example.

Notes: For optimum performance, be sure to connect your Wireless Voice Gateway to the first point the cable enters your home. The splitter must be rated for at least 1GHz.

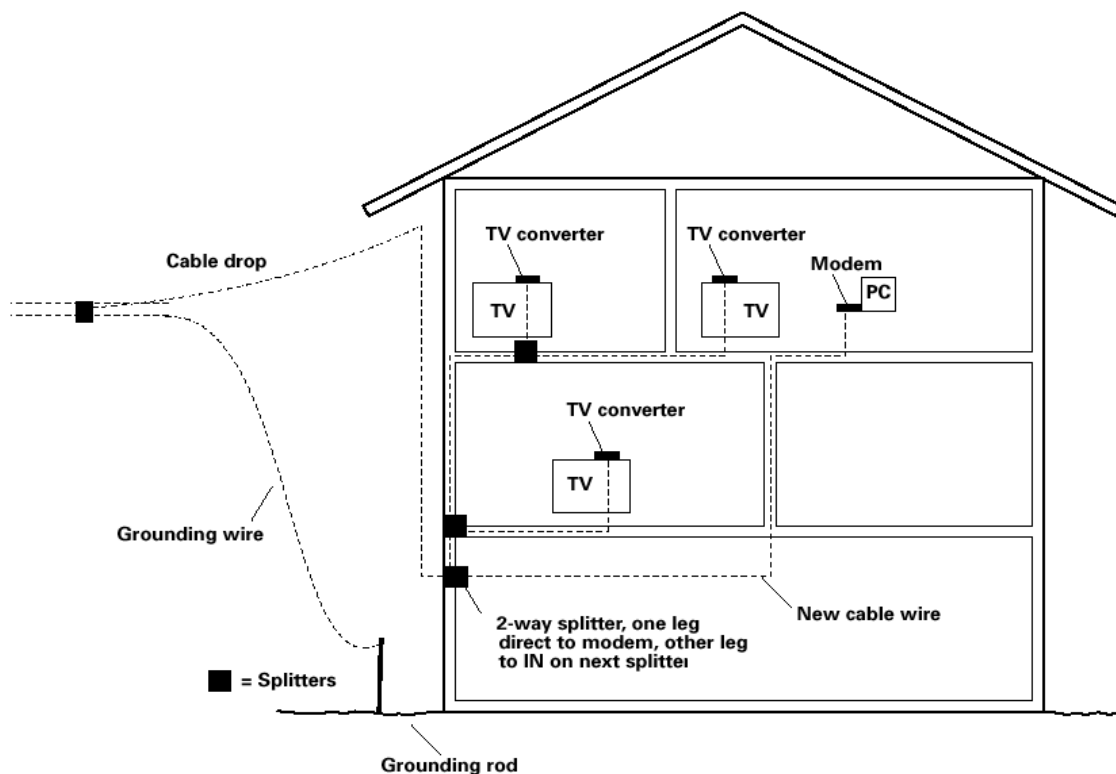


Fig. 1: Basic Home Wiring

Chapter 1: Connections and Setup

Important Connection Information

The Wireless Voice Gateway supports Ethernet connections simultaneously.

Below are important points to remember before you connect the Wireless Voice Gateway.

- For Ethernet connections, go to page 18.
- For telephone and fax connections, go to page 20.

Chapter 1: Connections and Setup

Ethernet Connection to a Computer

Make the connection to the modem in the following sequence:

1. Connect one end of the coaxial cable to the cable connection on the wall, and the other end to the CABLE jack on the Wireless Voice Gateway.
2. Connect the plug from the AC power supply into the POWER AC ADAPTER jack on the Wireless Voice Gateway, and plug the power supply into an AC outlet.

Note: Use only the power supply that accompanied this unit. Using other adapters may damage the unit.

3. Connect one end of the Ethernet cable to an Ethernet port on the back of your computer, and the other end to the ETHERNET port on the Wireless Voice Gateway.

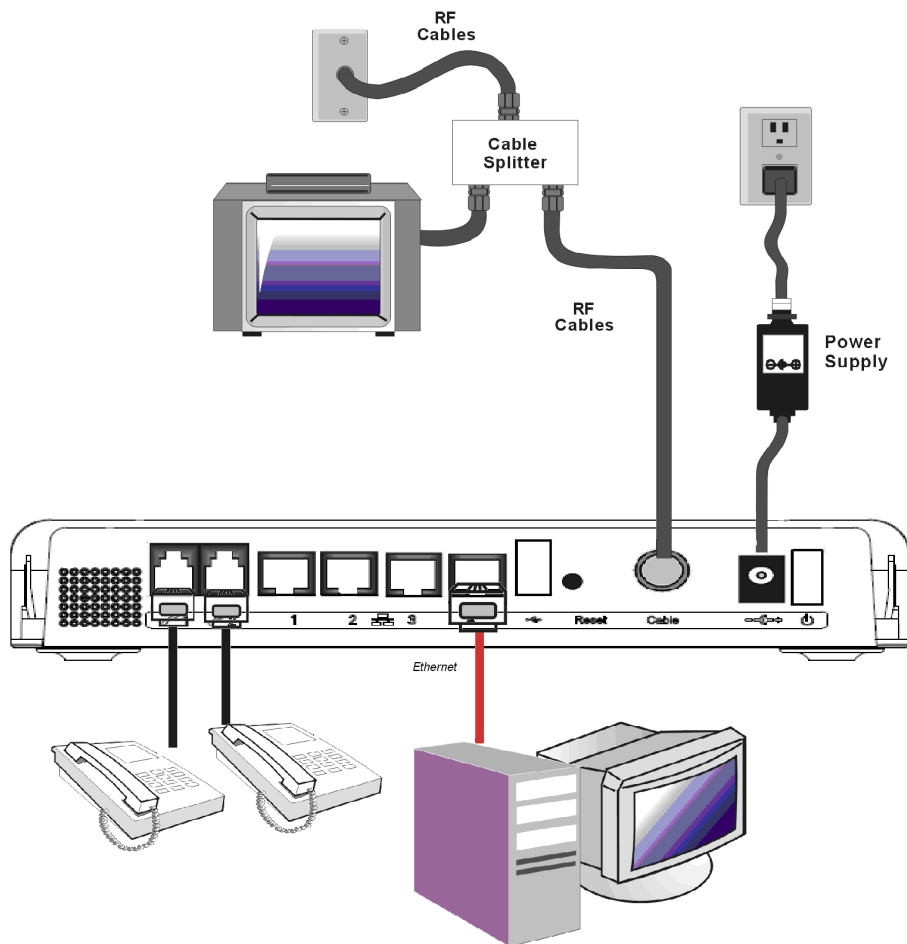


Fig.3: Ethernet Connection

Chapter 1: Connections and Setup

Connecting More Than A Computer to the Wireless Voice Gateway

If you need to connect more than one computer to the Wireless Voice Gateway, simply connect the computers to an Ethernet port on the rear panel.

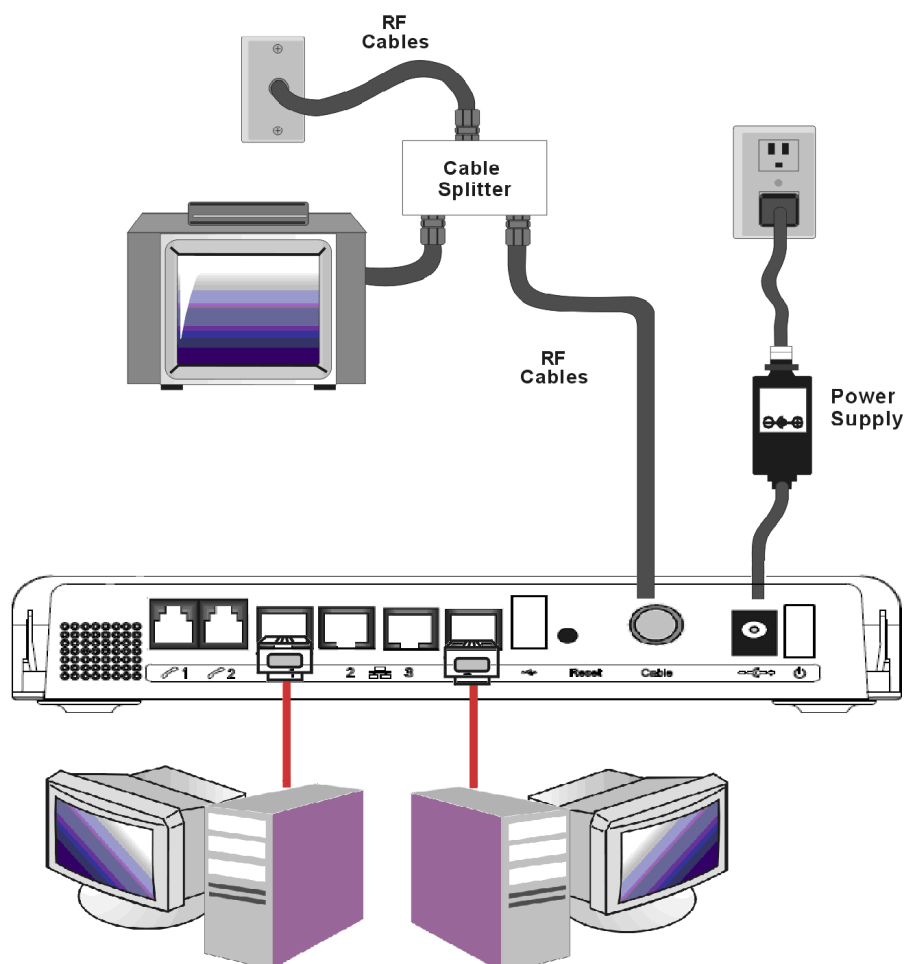


Fig.4: Multiple-PC Connection

Note: You may need to check with your service provider in order to connect multiple computers.

Chapter 1: Connections and Setup

Telephone or Fax Connection

When properly connected, most telephony devices can be used with the Wireless Voice Gateway just as with a conventional telephone service. To make a normal telephone call, pick up the handset; listen for a dial tone, then dial the desired number. For services such as call waiting, use the hook switch (or FLASH button) to change calls. The following procedures describe some of the possible connection schemes for using telephony devices with the Wireless Voice Gateway.

1. Connect a standard phone line cord directly from the phone (fax machine, answering machine, caller ID box, etc.) to one of the LINE jacks on the Wireless Voice Gateway.
2. If there is a phone line in your home which is NOT connected to another telephone service provider, connect a standard phone line cord from a jack on this line to one of the LINE jacks of the Wireless Voice Gateway. Connect a standard phone line cord directly from the phone (fax machine, answering machine, caller ID box, etc.) to one of the other jacks in the house that uses that line.
3. If you have a multi-line telephone, connect a standard phone line cord (not an RJ-14 type line cord) from the phone to the LINE jacks on the Wireless Voice Gateway. (Other phones can be added to each line by using standard phone line splitters.

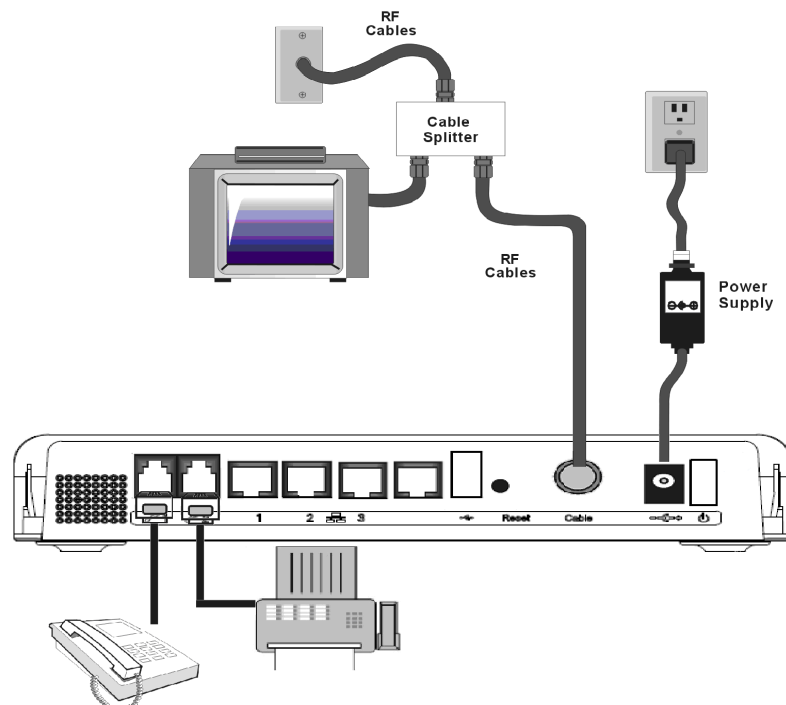


Fig. 5: Phone/Fax Connection

Chapter 2: WEB Configuration

Chapter 2: WEB Configuration

To make sure that you can access the Internet successfully, please check the following first.

1. Make sure the connection (through Ethernet) between the Wireless Voice Gateway and your computer is OK.
2. Make sure the TCP/IP protocol is set properly.
3. Subscribe to a Cable Company.

Accessing the Web Configuration

The **Wireless Voice Gateway** offers local management capability through a built-in HTTP server and a number of diagnostic and configuration web pages. You can configure the settings on the web page and apply them to the device.

Once your host PC is properly configured; please proceed as follows:

1. Start your web browser and type the private IP address of the Wireless Voice Gateway on the URL field: **192.168.0.1**.
2. After connecting to the device, you will be prompted to enter username and password. By default, the username is “ ” (empty) and the password is “**admin**”.



Fig. 6 Dialogue for Login

If you login successfully, the main page will appear.

Chapter 2: WEB Configuration

Outline of Web Manager

The main screen will be shown as below.

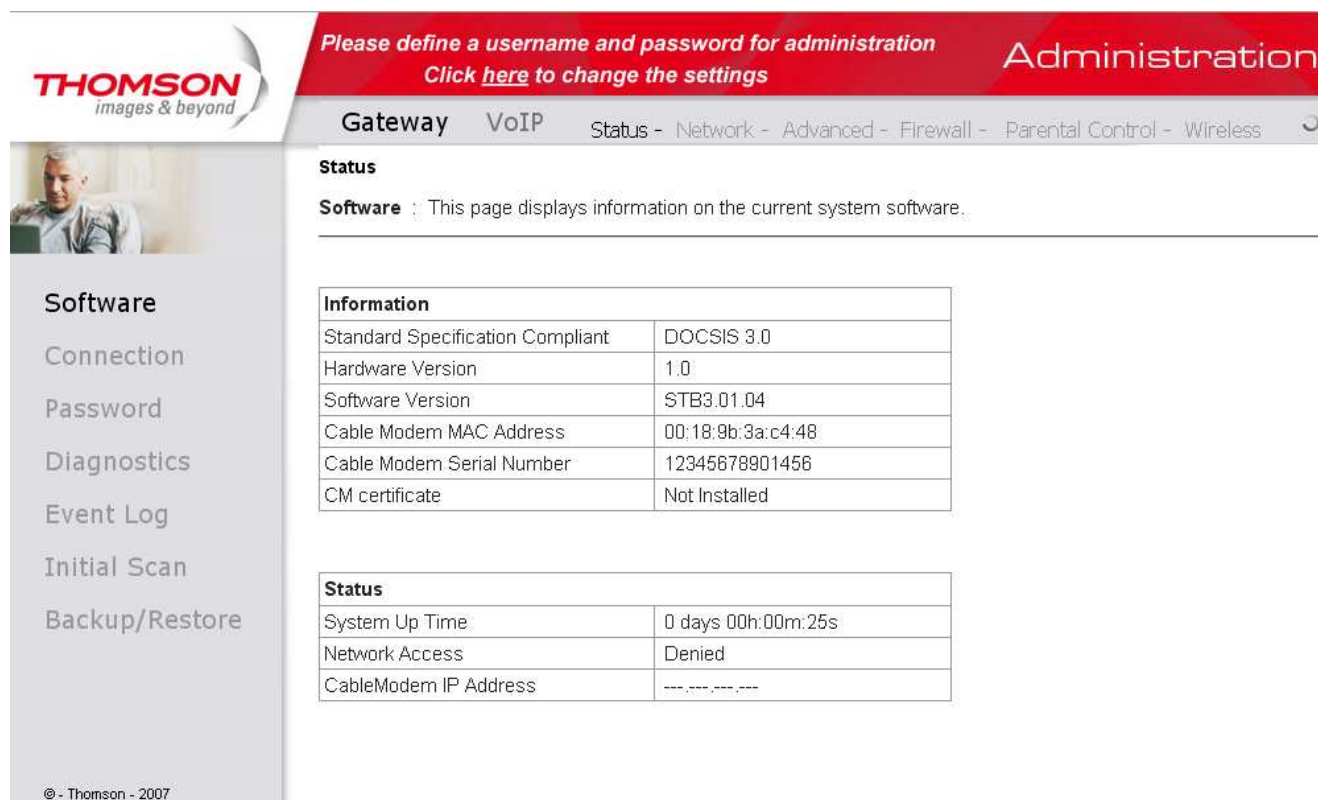


Fig. 7 Outline of Web Manager

- **Main Menu:** the hyperlinks on the top of the page, including Gateway, VoIP and several sub-menu items
- **Title:** the sidebar on the left side of the page indicates the title of this management interface, e.g., Software in this example
- **Main Window:** the current workspace of the web management, containing configuration or status information

For easy navigation, the pages are organized in groups with group in names main menu. Individual page names within each group are provided in the sidebar. So to navigate to a page, click the group hyperlink at the top, then the page title on the sidebar.

Your cable company may not support the reporting of some items of information listed on your gateway's internal web pages. In such cases, the information field appears blank. This is normal.

Chapter 2: WEB Configuration

Warning message to change the password

At your first connection or while the password is the default one, a warning message is displayed on the top banner of each Web configuration page. We want to encourage you to change the password in order to enforce the security of your modem. Please refer to the chapter “*Password*” page 27 for more information.

Chapter 2: WEB Configuration

Gateway – Status Web Page Group

1. Software

The information section shows the hardware and software information about your gateway.

The status section of this page shows how long your gateway has operated since last time being powered up, and some key information the Cable Modem received during the initialization process with your cable company. If Network Access shows “Allowed,” then your cable company has configured your gateway to have Internet connectivity. If not, you may not have Internet access, and should contact your cable company to resolve this.

The screenshot displays the Thomson Gateway Administration web interface. At the top, a red banner prompts the user to define a username and password for administration. Below this, a navigation bar includes links for Gateway, VoIP, Status, Network, Advanced, Firewall, Parental Control, and Wireless. The left sidebar contains a menu with options like Software, Connection, Password, Diagnostics, Event Log, Initial Scan, and Backup/Restore. The main content area is titled 'Status' and 'Software', indicating it displays current system software information. It contains two tables: 'Information' with details like Standard Specification Compliant (DOCSIS 3.0), Hardware Version (1.0), Software Version (STB3.01.04), Cable Modem MAC Address (00:18:9b:3a:c4:48), Cable Modem Serial Number (12345678901456), and CM certificate (Not Installed); and 'Status' with details like System Up Time (0 days 00h:00m:25s), Network Access (Denied), and CableModem IP Address (---.---.---).

Information	
Standard Specification Compliant	DOCSIS 3.0
Hardware Version	1.0
Software Version	STB3.01.04
Cable Modem MAC Address	00:18:9b:3a:c4:48
Cable Modem Serial Number	12345678901456
CM certificate	Not Installed



Status	
System Up Time	0 days 00h:00m:25s
Network Access	Denied
CableModem IP Address	---.---.---

Fig. 8 Gateway\Status\Software

Chapter 2: WEB Configuration

2. Connection

This page reports current connection status containing connection procedures, downstream and upstream status, CM online information, and so on. The information can be useful to your cable company's support technician if you're having problems.



Please define a username and password for administration
Click [here](#) to change the settings

Administration

Gateway VoIP Status - Network - Advanced - Firewall - Parental Control - Wireless

Status

Connection : This page displays information on the status of the cable modem's HFC and IP network connectivity.

Startup Procedure		
Procedure	Status	Comment
Acquire Downstream Channel		Locked
Connectivity State	OK	Operational
Boot State	OK	Operational
Configuration File	OK	
Security	Disabled	Disabled

Downstream Channels							
Channel	Lock Status	Modulation	Channel ID	Symbol rate	Frequency	Power	SNR
1	Locked	QAM256	2	5360537		46.7 dBmV	44.0 dB
2	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB
3	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB
4	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB
5	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB
6	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB
7	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB
8	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB

Upstream Channels						
Channel	Lock Status	Modulation	Channel ID	Symbol Rate	Frequency	Power
1	Locked	QAM64	2	2560 Ksym/sec		37.5 dBmV
2	Not Locked	Unknown	0	0 Ksym/sec		0.0 dBmV
3	Not Locked	Unknown	0	0 Ksym/sec		0.0 dBmV
4	Not Locked	Unknown	0	0 Ksym/sec		0.0 dBmV

CM IP Address	Duration	Expires
---	D: -- H: -- M: -- S: --	---

Current System Time: Tue Dec 15 09:58:41 2009

Software
Connection
Password
Diagnostics
Event Log
Initial Scan
Backup/Restore

© - Thomson - 2007

Fig. 9 Gateway\Status\Connection

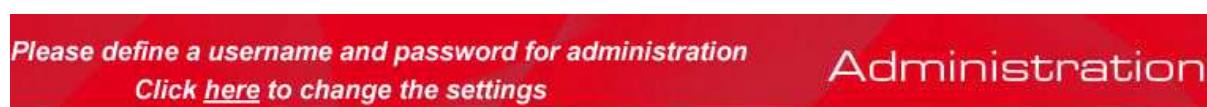
Chapter 2: WEB Configuration

3. Password

Forcing end user to change the password

Upon access to the web pages on the CPE side of the router, if the user has not changed the default web password, a warning message must be displayed in the top banner of the web interface such as being visible while accessing any tabs.

This warning message informs the user that the default password must be changed:



In the second sentence, “here” is a hyperlink to the password setting page. Clicking on “here” lead to the display of the password setting page.

More information

By default, the username is empty (“”) and the password is “admin”.

This is set by different actions (non exhaustive list):

- at the manufactory level,
- following a reset factory on the modem,
- following a reset from the operator,
- following a change by the user who wants to come back to the default setting after using its own settings

When the current password is the default one, the user is strongly encouraged to change the default web password.

At your first connection or while the password is the default one, a warning message is displayed on the top banner of each Web configuration page. We want to encourage you to change the password in order to enforce the security of your modem.

The password can be a maximum of 8 characters and is case sensitive. In addition, this page can be used to restore the gateway to its original factory settings. Use this with caution, as all the settings you have made will be lost. To perform this reset, set **Restore Factory Defaults** to **Yes** and click **Apply**. This has the same effect as a factory reset using the rear panel reset switch, where you hold on the switch for 15 seconds, then release it.

Note: We are always suggesting to modify the password. This is a basic protection against wrongful access to the Gateway Web pages.

Chapter 2: WEB Configuration

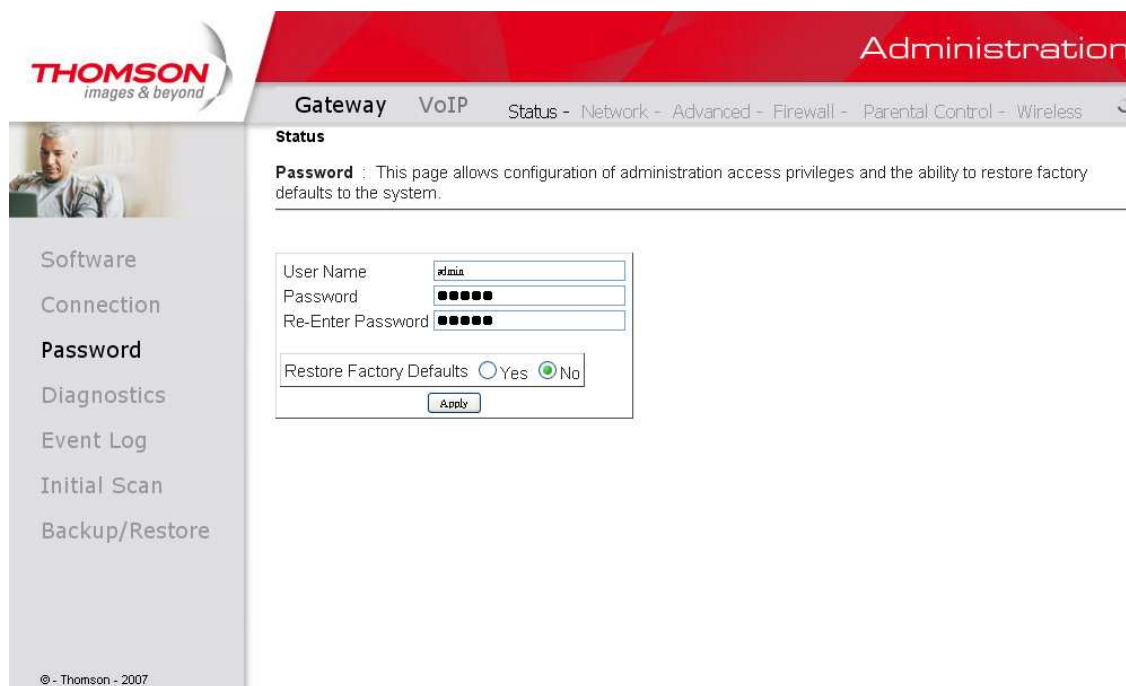
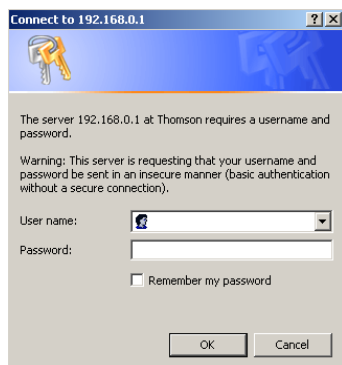


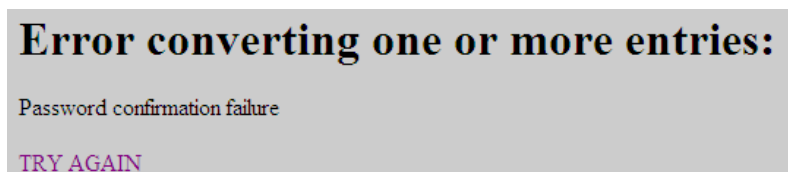
Fig. 10 Gateway\Status\Password

To change the password: type the password, and re-enter it again.

If the password is accepted, you are required to re log on the web pages:



If the password is no accepted, an error message is displayed:



Click on try again.

Chapter 2: WEB Configuration

4. Diagnostics

This page offers basic diagnostic tools for you to utilize when connectivity problems occur. When you ping an Internet device, you send a packet to its TCP/IP stack, and it sends one back to yours. To use the ping Test, enter the information needed and press **Start Test**; the Result will be displayed in the lower part of the window. Press **Abort Test** to stop, and **Clear Results** to clear the result contents.

Note: Firewalls may cause pings to fail but still provide you TCP/IP access to selected devices behind them. Keep this in mind when pinging a device that may be behind a firewall. Ping is most useful to verify connectivity with PCs which do not have firewalls, such as the PCs on your LAN side.

THOMSON
images & beyond

Administration

Gateway VoIP Status - Network - Advanced - Firewall - Parental Control - Wireless

Status

Diagnostics : This page provides for ping diagnostics to the LAN to help with IP connectivity problems.

Ping Test Parameters

Ping Target

Ping Size bytes

No. of Pings

Ping Interval ms

Results

Waiting for input...

To get an update of the results you must REFRESH the page.

© - Thomson - 2007

Fig. 11 Gateway\Status\Diagnostics

Chapter 2: WEB Configuration

5. Event Log

This page displays the contents of the SNMP event log. Press “**Clear Log**” button to clear the logs.

The screenshot shows the Thomson Gateway Administration web interface. The top navigation bar includes 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Status' section is active, displaying the 'SNMP Event Log'. A sidebar on the left contains links for 'Software', 'Connection', 'Password', 'Diagnostics', 'Event Log', 'Initial Scan', and 'Backup/Restore'. The main content area shows a table of event logs with columns for Time, Priority, and Description. A 'Clear Log' button is located below the table.

Time	Priority	Description
Wed Oct 21 11:02:53 2009	Critical (3)	Resetting the cable modem due to docsDevResetNow
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire FEC f...
Tue Oct 20 22:26:09 2009	Critical (3)	No Ranging Response received - T3 time-out; CM-MAC=00:18:9b:3a...
Tue Oct 20 22:26:14 2009	Critical (3)	TFTP failed - Request sent - No Response; CM-MAC=00:18:9b:3a:c...
Tue Oct 20 22:24:25 2009	Critical (3)	DHCP FAILED - Discover sent, no offer received; CM-MAC=00:18:9...
Tue Oct 20 22:19:19 2009	Critical (3)	Started Unicast Maintenance Ranging - No Response received - ...

Clear Log

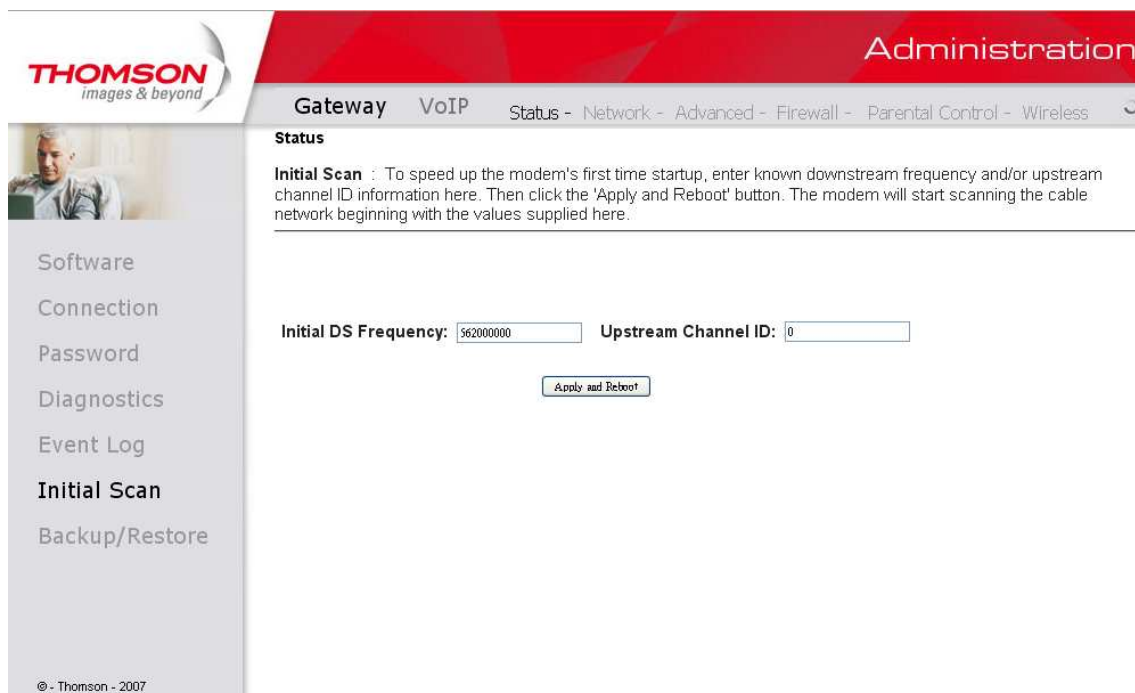
Fig. 12 Gateway\Status\Event Log

Chapter 2: WEB Configuration

6. Initial Scan

To speed up the modem's first time connection, enter known downstream frequency and/or upstream channel ID information here. Then click **“Apply and Reboot”** button to start scanning the cable network beginning with the values supplied here.

The value is provided in Hertz. So for 562 MHz, you must type: 562000000



The screenshot shows the Thomson Gateway Administration web interface. The top navigation bar includes 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Status' tab is selected. On the left sidebar, the 'Initial Scan' option is highlighted. The main content area is titled 'Initial Scan' and contains a descriptive paragraph: 'To speed up the modem's first time startup, enter known downstream frequency and/or upstream channel ID information here. Then click the 'Apply and Reboot' button. The modem will start scanning the cable network beginning with the values supplied here.' Below this text are two input fields: 'Initial DS Frequency' with the value '562000000' and 'Upstream Channel ID' with the value '0'. An 'Apply and Reboot' button is located below these fields. The Thomson logo and copyright notice '© - Thomson - 2007' are visible in the bottom left corner.

Fig. 13 Gateway\Status\Initial Scan

Chapter 2: WEB Configuration

7. Backup/Restore

Backup/Restore Settings : This page allows you to save your current settings locally on your PC, or restore settings previously saved. The default file name is “GatewaySettings.bin”.

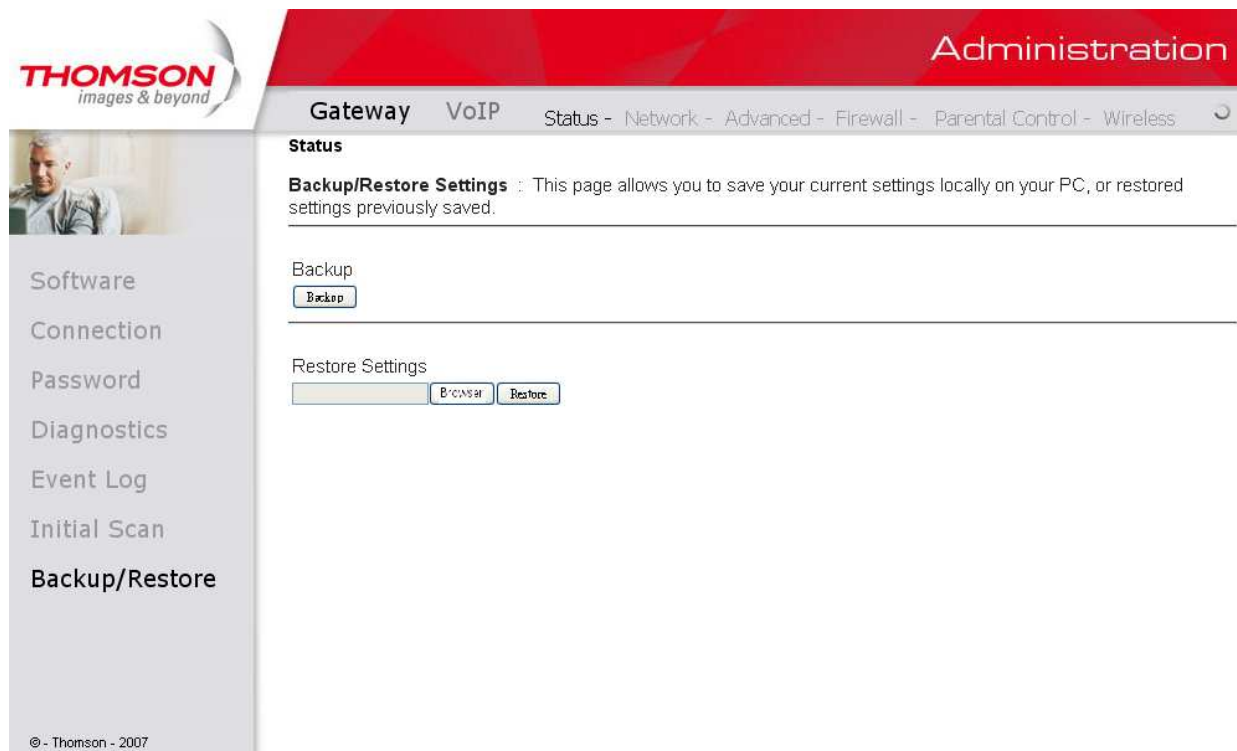


Fig 14 Gateway\Status\Backup/Restore

Chapter 2: WEB Configuration

Gateway – Network Web Page Group

1. LAN

You can activate the DHCP server function for the LAN on this page.

With this activated function,

- your cable company's DHCP server provides one IP address for your gateway,
- and your gateway's DHCP server provides IP addresses, starting at the address you set in IP Address on the LAN page, to your PCs. A DHCP server leases an IP address with an expiration time.

To change the IP address that your gateway will use on the LAN side, enter it into the **IP Address** box and then click **Apply**.

IP Address and Subnet Mask:

A private IP address and Subnet Mask for LAN sub netting.

For example 192.168.0.1 / 255.255.255.0.

DHCP Server:

- Select the check point of “Yes” or “No” to enable or disable a simple DHCP server for LAN.
- Configure the IP address numbers for the DHCP server with “lease pool start” and “lease pool end”.
- Configure the IP address lease time with “lease time” for DHCP server. Default value is 604800 seconds.

The screenshot shows the Thomson Gateway Administration interface. The top navigation bar includes 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Network' section is active, showing 'LAN' configuration. The 'Network Configuration' section includes fields for IP Address (192.168.0.1), Subnet Mask (255.255.255.0), and MAC Address (00:18:9b:3a:c4:4c). The DHCP Server is enabled (Yes), and the Lease Pool Start is 192.168.0.10, Lease Pool End is 192.168.0.254, and Lease Time is 604800 seconds. An 'Apply' button is at the bottom.

Fig. 15 Gateway\Network\LAN

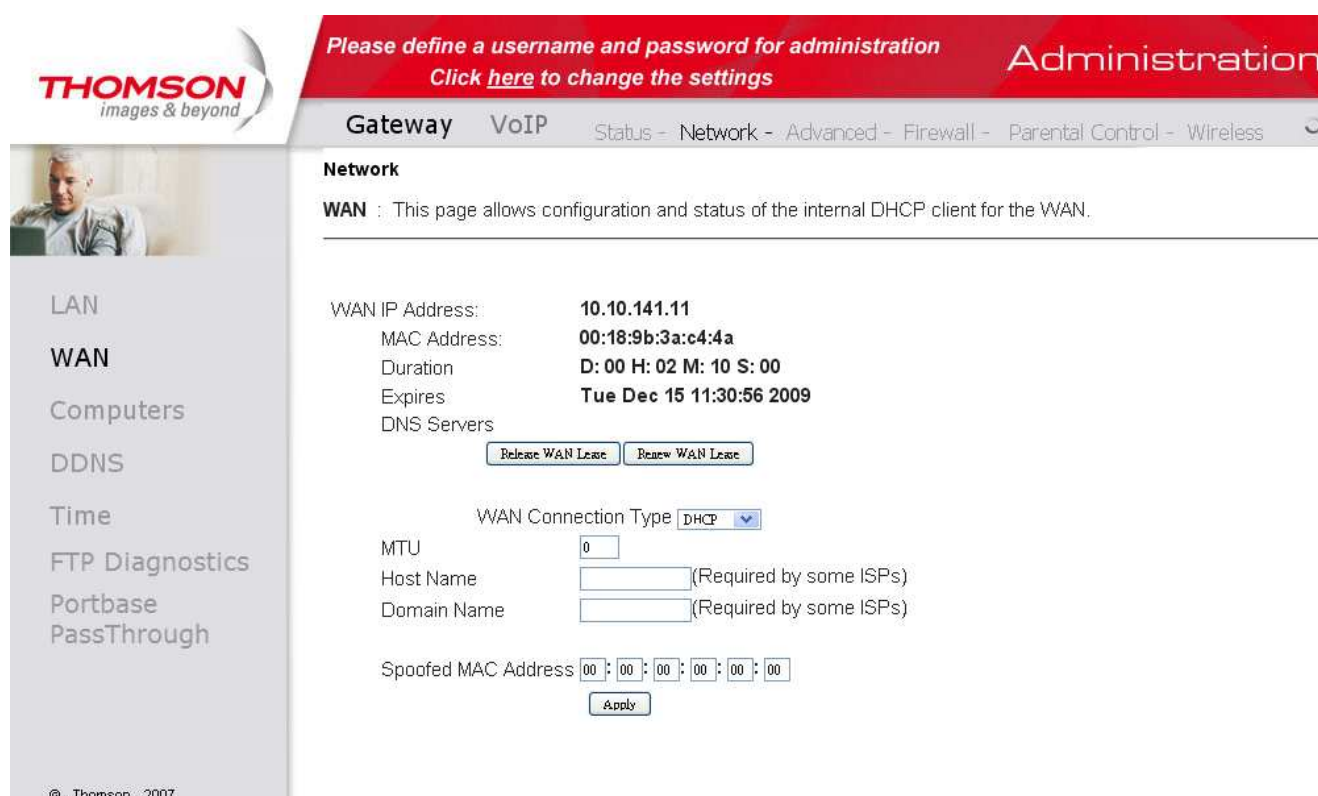
Chapter 2: WEB Configuration

2. WAN

You can configure the optional internal DHCP server for the WAN on this page. This can be required by some ISP providers.

Select different WAN Connection Type will lead to different contents. Take the WAN connection type-DHCP for example, you can release and renew the WAN lease by pressing the buttons.

You can enter a spoofed MAC address that causes your gateway networking stack to use that MAC address when communicating instead of the usual WAN MAC address, e.g., if the MAC address is 00:11:e3:df:66:95, this spoofed MAC address could be 00:11:e3:df:66:97 or any desired MAC address.



The screenshot shows the Thomson Gateway Administration interface. The top navigation bar includes 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Network' section is active, displaying the 'WAN' configuration page. The page title is 'Please define a username and password for administration' with a link to 'Click here to change the settings'. The 'WAN' section explains that it allows configuration and status of the internal DHCP client for the WAN. The configuration fields include: WAN IP Address (10.10.141.11), MAC Address (00:18:9b:3a:c4:4a), Duration (D: 00 H: 02 M: 10 S: 00), Expires (Tue Dec 15 11:30:56 2009), and DNS Servers. There are buttons for 'Release WAN Lease' and 'Renew WAN Lease'. The 'WAN Connection Type' is set to 'DHCP'. The 'MTU' is set to '0'. The 'Host Name' and 'Domain Name' fields are empty, with a note '(Required by some ISPs)'. The 'Spoofed MAC Address' field is empty, with a note '(Required by some ISPs)'. There is an 'Apply' button at the bottom.

THOMSON
images & beyond

Please define a username and password for administration
Click [here](#) to change the settings

Administration

Gateway VoIP Status - Network - Advanced - Firewall - Parental Control - Wireless

Network

WAN : This page allows configuration and status of the internal DHCP client for the WAN.

WAN IP Address: 10.10.141.11
MAC Address: 00:18:9b:3a:c4:4a
Duration: D: 00 H: 02 M: 10 S: 00
Expires: Tue Dec 15 11:30:56 2009
DNS Servers

Release WAN Lease Renew WAN Lease

WAN Connection Type: DHCP

MTU: 0

Host Name: (Required by some ISPs)

Domain Name: (Required by some ISPs)

Spoofed MAC Address: 00:00:00:00:00:00

Apply

© - Thomson - 2007

Fig. 16 Gateway\Network\WAN

Chapter 2: WEB Configuration

3. Computers

This page displays the status of the DHCP clients and current system time. You can cancel an IP address lease by selecting it in the DHCP Client Lease Info list and then clicking the Force Available button. If you do so, you may have to perform a DHCP Renew on that PC, so that it can obtain a new lease.

THOMSON
images & beyond

Please define a username and password for administration
Click [here](#) to change the settings

Administration

Gateway VoIP Status - Network - Advanced - Firewall - Parental Control - Wireless

Network

Computers : This page shows the status of the DHCP clients and current system time.

DHCP Clients

MAC Address	IP Address	Subnet Mask	Duration	Expires	Select
0013d43b6fd3	192.168.000.010	255.255.255.000	D:07 H:00 M:00 S:00	Tue Dec 22 10:19:00 2009	<input type="radio"/>

Current System Time: Tue Dec 15 10:19:31 2009

[Force Available](#)

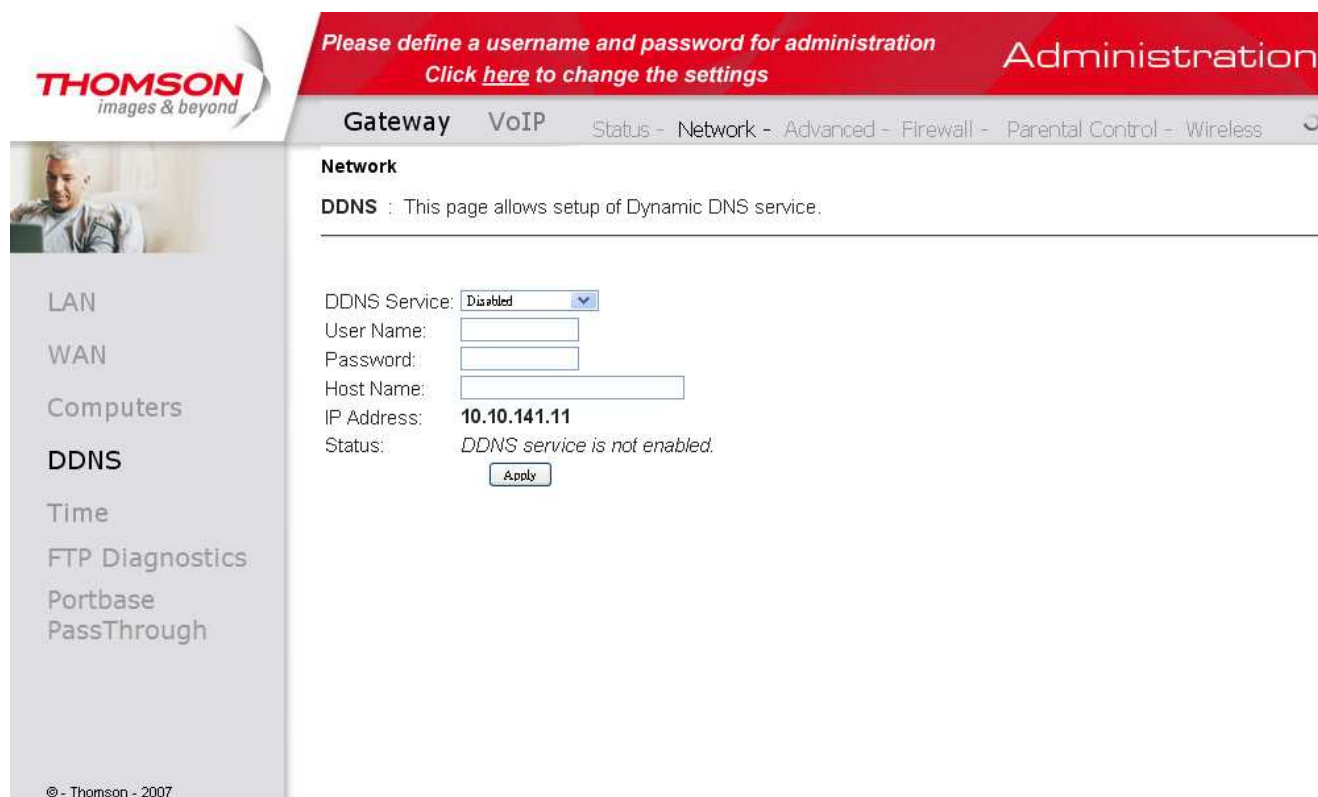
© - Thomson - 2007

Fig. 17 Gateway\Network\Computers

Chapter 2: WEB Configuration

4. DDNS - Dynamic DNS service

This page allows to setup for Dynamic DNS server.



The screenshot shows the Thomson Gateway Administration interface. At the top, a red banner reads "Please define a username and password for administration" and "Click [here](#) to change the settings". The "Administration" title is on the right. Below the banner, a navigation bar includes "Gateway", "VoIP", "Status", "Network", "Advanced", "Firewall", "Parental Control", and "Wireless". The "Network" tab is selected. On the left, a sidebar lists "LAN", "WAN", "Computers", "DDNS", "Time", "FTP Diagnostics", "Portbase", and "PassThrough". The "DDNS" option is highlighted. The main content area is titled "Network" and "DDNS : This page allows setup of Dynamic DNS service." It contains the following fields: "DDNS Service:" with a dropdown menu set to "Disabled", "User Name:" with an empty text box, "Password:" with an empty text box, "Host Name:" with an empty text box, "IP Address:" with the value "10.10.141.11", and "Status:" with the text "DDNS service is not enabled." and an "Apply" button. The Thomson logo "THOMSON images & beyond" is in the top left corner, and "© - Thomson - 2007" is at the bottom left.

Fig 18 Gateway\Network\DDNS

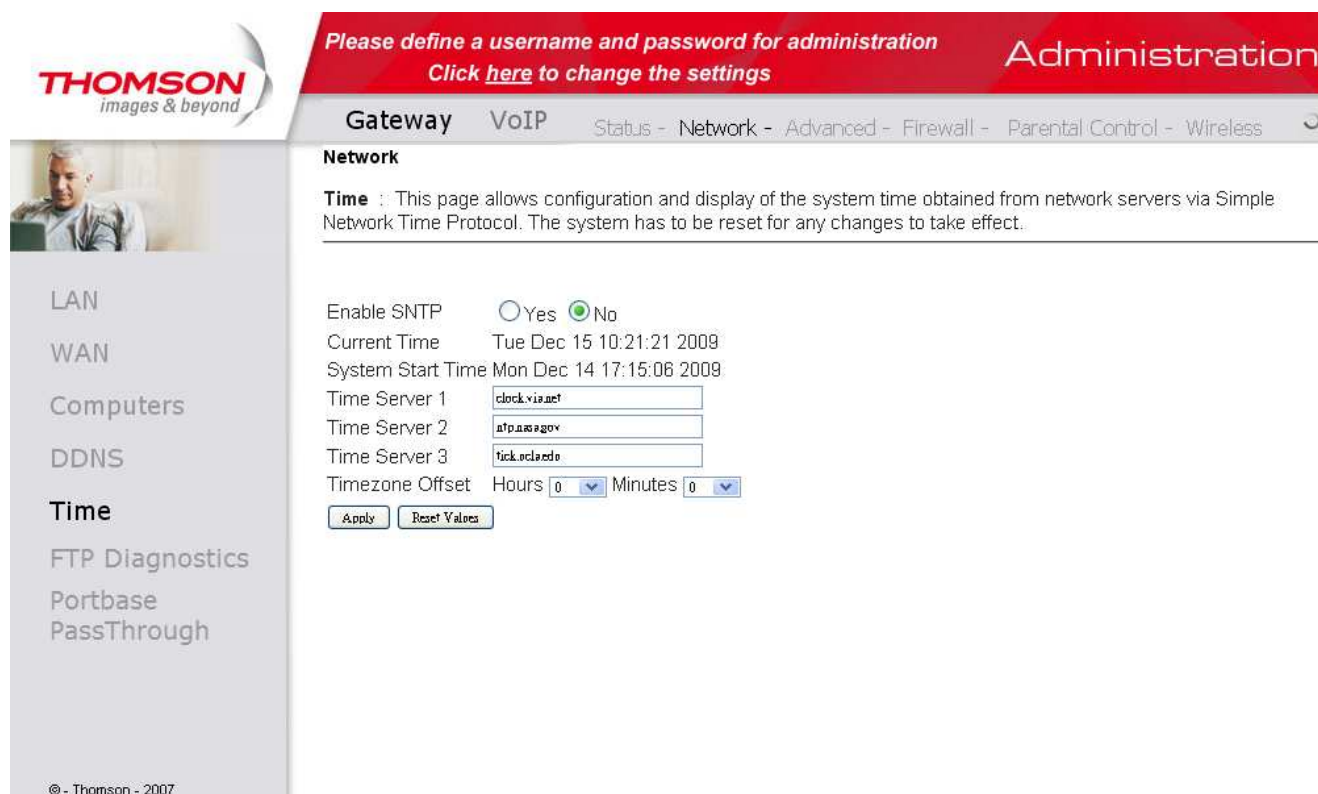
- **DDNS Service-** Choose Enabled (www.DynDNS.org) to enable the basic setting. Choose Disabled to close the basic setting.
- **Username-** The username that you registered with your DDNS provider.
- **Password-** The password that you registered with your DDNS provider
- **Host Name-** The domain name or host name that is registered with your DDNS provider
- **Status-** It shows the DDNS service status whether it is enabled or disabled.

Click Apply to save the changes

Chapter 2: WEB Configuration

5. Time server

This page allows configuration and display of the system time obtained from network servers via Simple Network Time Protocol. The system has to be reset for any changes to take effect.



The screenshot displays the Thomson Gateway Administration web interface. The top navigation bar is red with the text "Please define a username and password for administration" and "Click here to change the settings". The "Administration" title is on the right. Below the navigation bar, a menu shows "Gateway" selected, with other options like "VoIP", "Status", "Network", "Advanced", "Firewall", "Parental Control", and "Wireless". The "Network" section is active, showing a "Time" configuration page. The page content includes a description of the Simple Network Time Protocol (SNTP) and fields for enabling SNTP, displaying the current time, system start time, and three time servers. The "Timezone Offset" is set to 0 hours and 0 minutes. "Apply" and "Reset Values" buttons are at the bottom.

THOMSON
images & beyond

Please define a username and password for administration
Click here to change the settings

Administration

Gateway VoIP Status - Network - Advanced - Firewall - Parental Control - Wireless

Network

Time : This page allows configuration and display of the system time obtained from network servers via Simple Network Time Protocol. The system has to be reset for any changes to take effect.

Enable SNTP ☐ Yes ☒ No

Current Time Tue Dec 15 10:21:21 2009

System Start Time Mon Dec 14 17:15:06 2009

Time Server 1 clock.via.net

Time Server 2 atp.moscow

Time Server 3 tick.nclazdo

Timezone Offset Hours 0 Minutes 0

Apply Reset Values

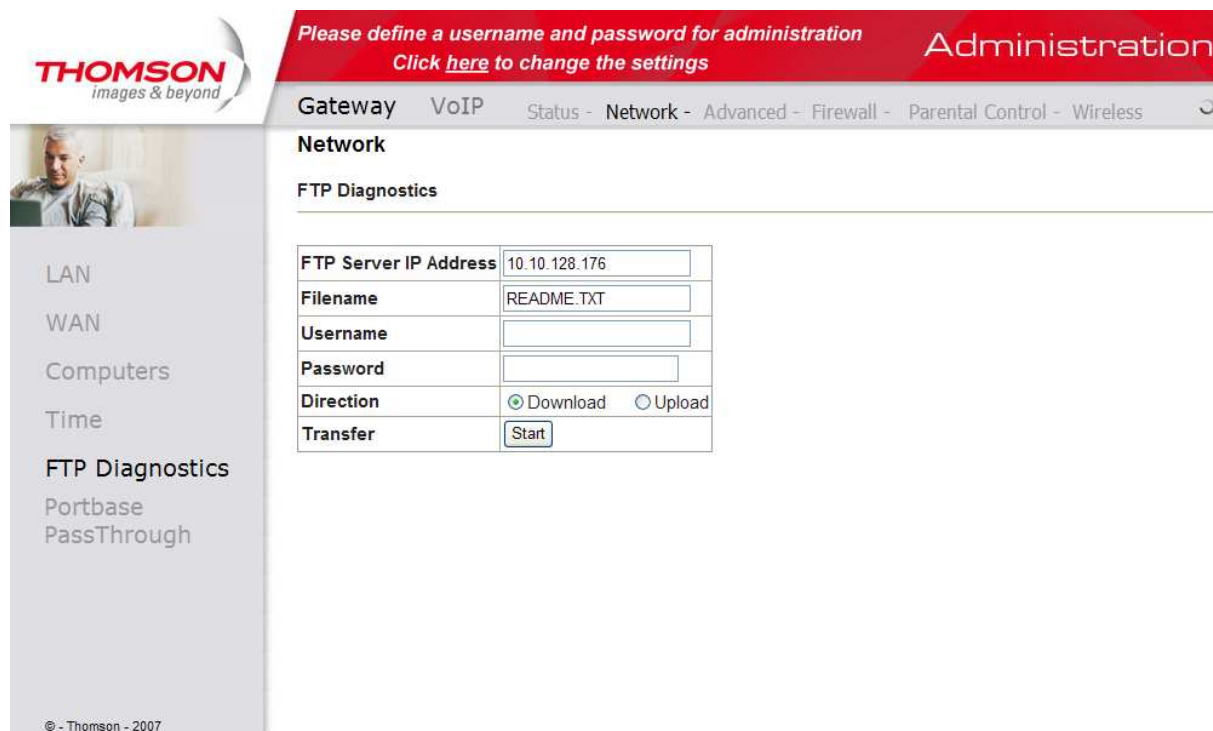
© - Thomson - 2007

Fig 19 Gateway\Network\Time

Chapter 2: WEB Configuration

6. FTP Diagnostics

You can test throughput performance via FTP in this page. Choose the FTP Server to get a file, during Downloading or Uploading system will calculate Payload Data Bytes, Total Packet Bytes and Elapsed Time to gain Payload Throughput and Packet Throughput.

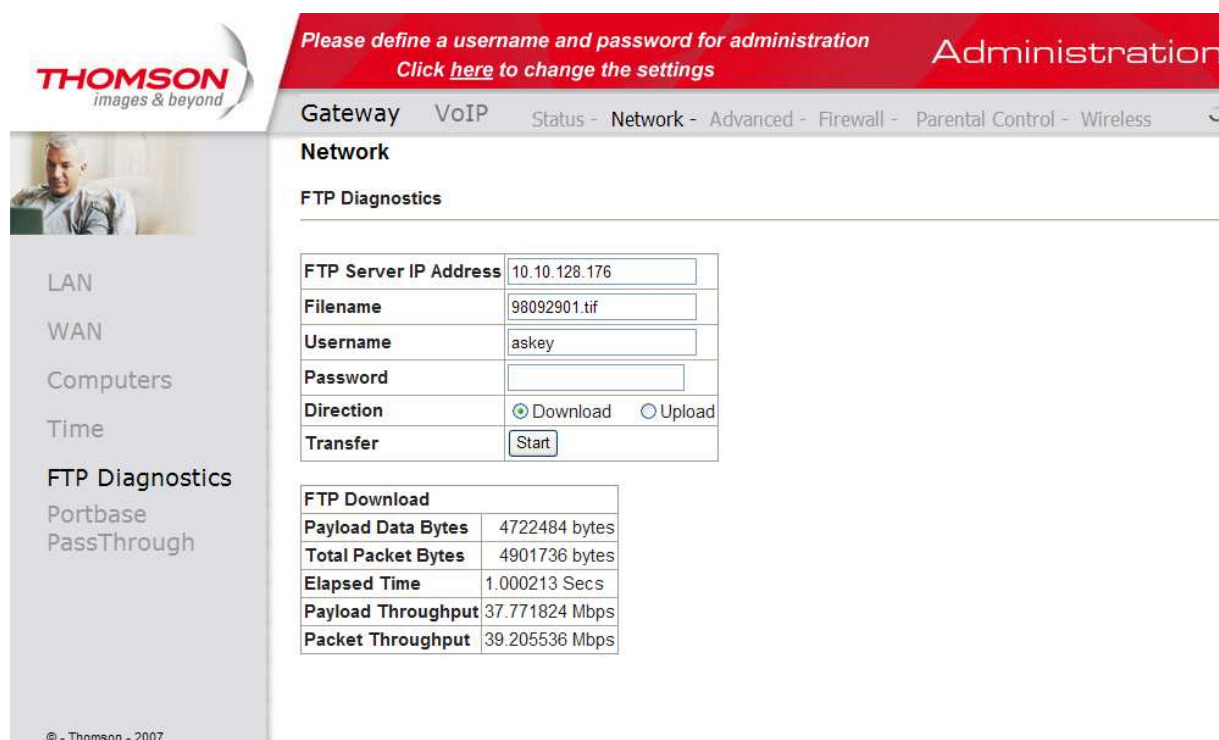


The screenshot shows the Thomson Gateway Administration interface. The top navigation bar includes 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Network' section is selected, and the 'FTP Diagnostics' sub-section is active. The form contains the following fields:

FTP Server IP Address	10.10.128.176
Filename	README.TXT
Username	
Password	
Direction	<input checked="" type="radio"/> Download <input type="radio"/> Upload
Transfer	<input type="button" value="Start"/>

The left sidebar shows a menu with options: LAN, WAN, Computers, Time, FTP Diagnostics (selected), Portbase, and PassThrough. The Thomson logo and copyright notice '© - Thomson - 2007' are also visible.

Fig 20-1 Gateway\Network\FTP Diagnostics



This screenshot shows the same Thomson Gateway Administration interface as Fig 20-1, but with the 'FTP Diagnostics' results displayed. The configuration fields are the same, but the 'Transfer' button is now disabled. Below the configuration fields, a table shows the results of the FTP download:

FTP Download	
Payload Data Bytes	4722484 bytes
Total Packet Bytes	4901736 bytes
Elapsed Time	1.000213 Secs
Payload Throughput	37.771824 Mbps
Packet Throughput	39.205536 Mbps

The rest of the interface, including the navigation bar and sidebar, remains the same as in Fig 20-1.

Fig 20-2 Gateway\Network\FTP Diagnostics

Chapter 2: WEB Configuration

7. Portbase PassThrough

This page allows configuration of Portbase PassThrough. After you enable it, which Ethernet port will get public IP without NAT.

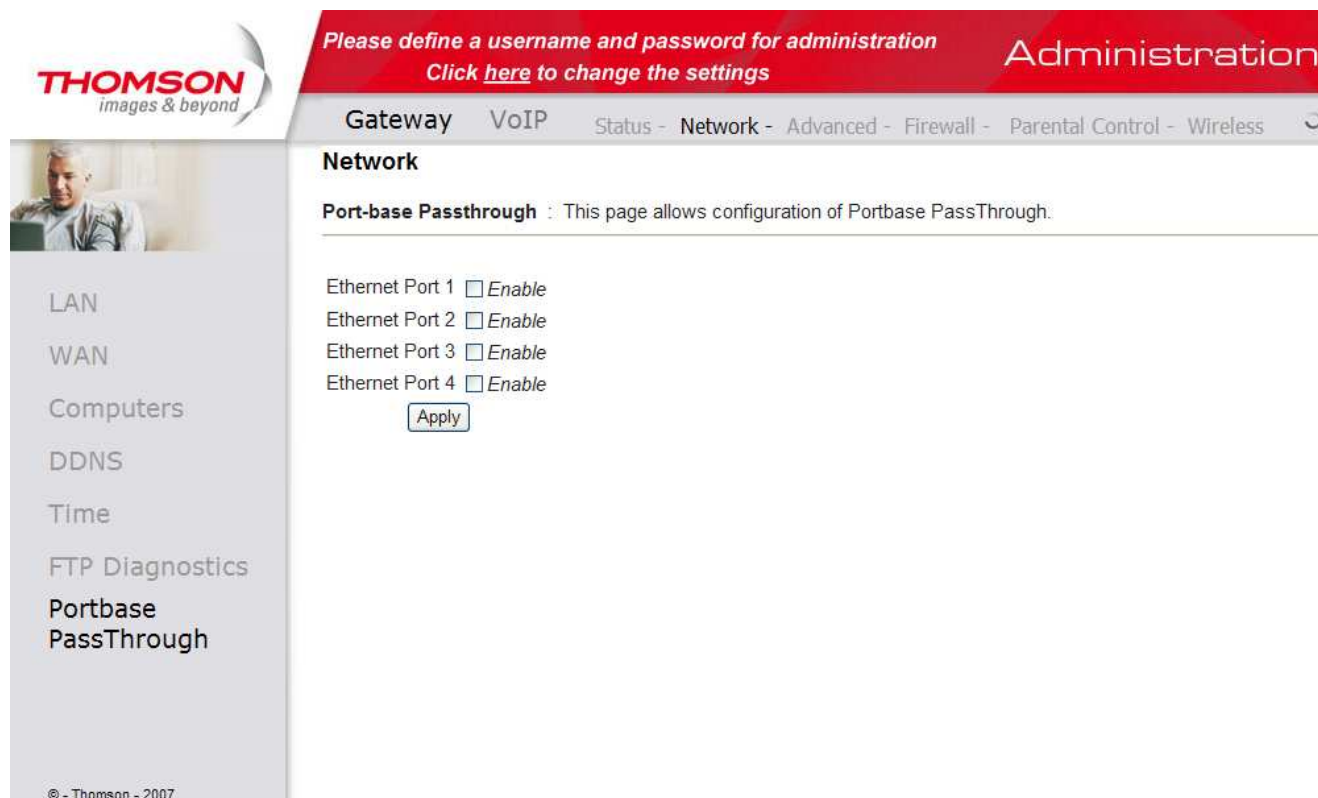


Fig 21 Gateway\Network\Portbase PassThrough

Chapter 2: WEB Configuration

Gateway – Advanced Web Page Group

1. Options

This page allows you to enable/disable some features of the Wireless Voice Gateway.

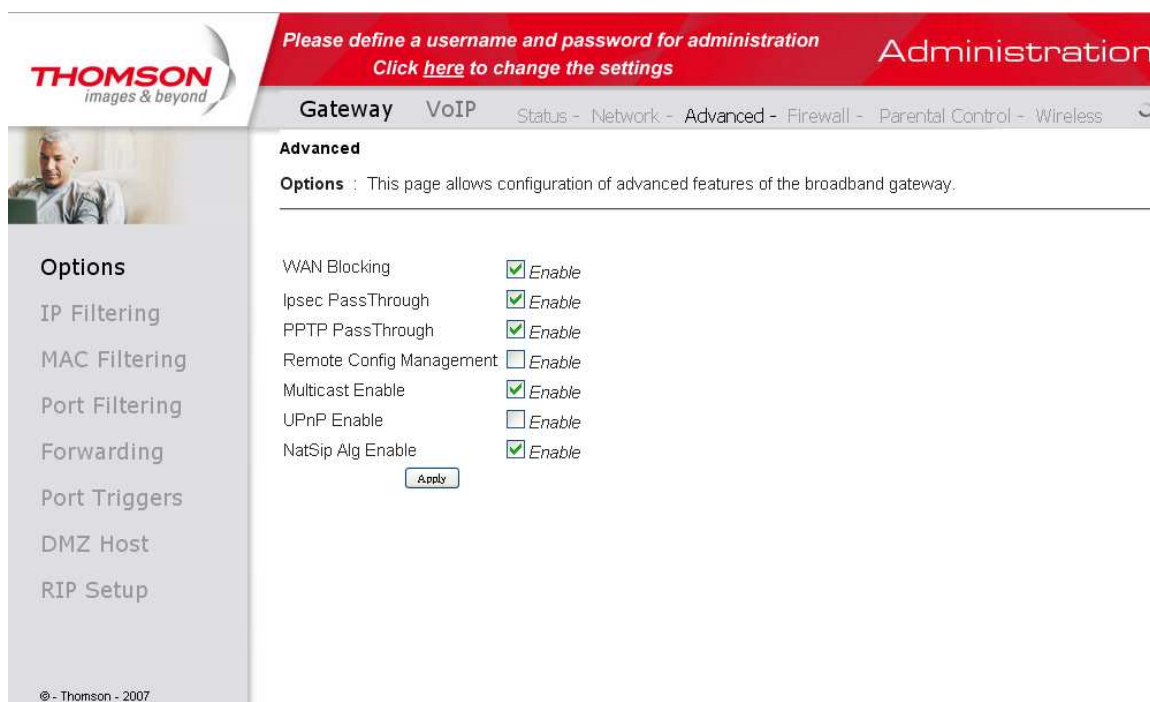


Fig. 22 Gateway\Advanced\Options

- **WAN Blocking** prevents others on the WAN side from being able to ping your gateway. With WAN Blocking enabled, your gateway will not respond to pings it receives, effectively “hiding” your gateway.
- **Ipsec PassThrough** enables IpSec type packets to pass WAN ⇔ LAN. IpSec (IP Security) is a security mechanism used in Virtual Private Networks (VPNs).
- **PPTP PassThrough** enables PPTP type packets to pass WAN ⇔ LAN. PPTP (Point to Point Tunneling Protocol) is another mechanism sometimes used in VPNs.
- **Remote Config Management** makes the configuration web pages in your gateway accessible from the WAN side. Note that page access is limited to only those who know the gateway access password. When accessing your gateway from a remote location, you must use HTTP port 8080 and the WAN IP address of the gateway. For example, if the WAN IP address is 157.254.5.7, you would navigate to <http://157.254.5.7:8080> to reach your gateway.
- **Multicast Enable** enables multicast traffic to pass WAN⇔ LAN. You may need to enable this to see some types of broadcast streaming and content on the Internet.
- **UPnP** Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically

Chapter 2: WEB Configuration

discover the services from other registered UPnP devices on the network.

- **NatSipAlg Enable** the gateway implements SIP ALG (Application-level gateway). It is enabled by default and help in solving NAT related problems in client LAN side.

Chapter 2: WEB Configuration

2. IP Filtering

This page enables you to enter the IP address ranges of PCs on your LAN that you don't want to have outbound access to the WAN. These PCs can still communicate with each other on your LAN, but packets they send to WAN addresses are blocked by the gateway.

THOMSON
images & beyond

Administration

Gateway VoIP Status - Network - Advanced - Firewall - Parental Control - Wireless

Advanced

IP Filtering : This page allows the configuration of IP Address filters in order to block internet traffic to specific network devices on the LAN.

IP Filtering		
Start Address	End Address	Enabled
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>

Apply

Options
IP Filtering
MAC Filtering
Port Filtering
Forwarding
Port Triggers
DMZ Host
RIP Setup

© - Thomson - 2007

Fig. 23 Gateway\Advanced\IP Filtering

Chapter 2: WEB Configuration

3. MAC Filtering

This page enables you to enter the MAC address of specific PCs on your LAN that you do not wish to have outbound access to the WAN. As with IP filtering, these PCs can still communicate with each other through the gateway, but packets they send to WAN addresses are blocked.

The screenshot shows the Thomson Gateway Administration interface. The top navigation bar includes 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced' (selected), 'Firewall', 'Parental Control', and 'Wireless'. The left sidebar lists various configuration options, with 'MAC Filtering' highlighted. The main content area is titled 'Advanced' and contains a description of the MAC Filtering feature. Below this is a table for 'MAC Address Filters' with 20 rows, each containing a MAC address field. An 'Apply' button is located at the bottom of the table.

THOMSON
images & beyond

Administration

Gateway VoIP Status - Network - **Advanced** - Firewall - Parental Control - Wireless

Advanced

MAC Filtering : This page allows configuration of MAC Address filters in order to block internet traffic to specific network devices on the LAN.

MAC Address Filters	
MAC 01	00:00:00:00:00:00
MAC 02	00:00:00:00:00:00
MAC 03	00:00:00:00:00:00
MAC 04	00:00:00:00:00:00
MAC 05	00:00:00:00:00:00
MAC 06	00:00:00:00:00:00
MAC 07	00:00:00:00:00:00
MAC 08	00:00:00:00:00:00
MAC 09	00:00:00:00:00:00
MAC 10	00:00:00:00:00:00
MAC 11	00:00:00:00:00:00
MAC 12	00:00:00:00:00:00
MAC 13	00:00:00:00:00:00
MAC 14	00:00:00:00:00:00
MAC 15	00:00:00:00:00:00
MAC 16	00:00:00:00:00:00
MAC 17	00:00:00:00:00:00
MAC 18	00:00:00:00:00:00
MAC 19	00:00:00:00:00:00
MAC 20	00:00:00:00:00:00

Apply

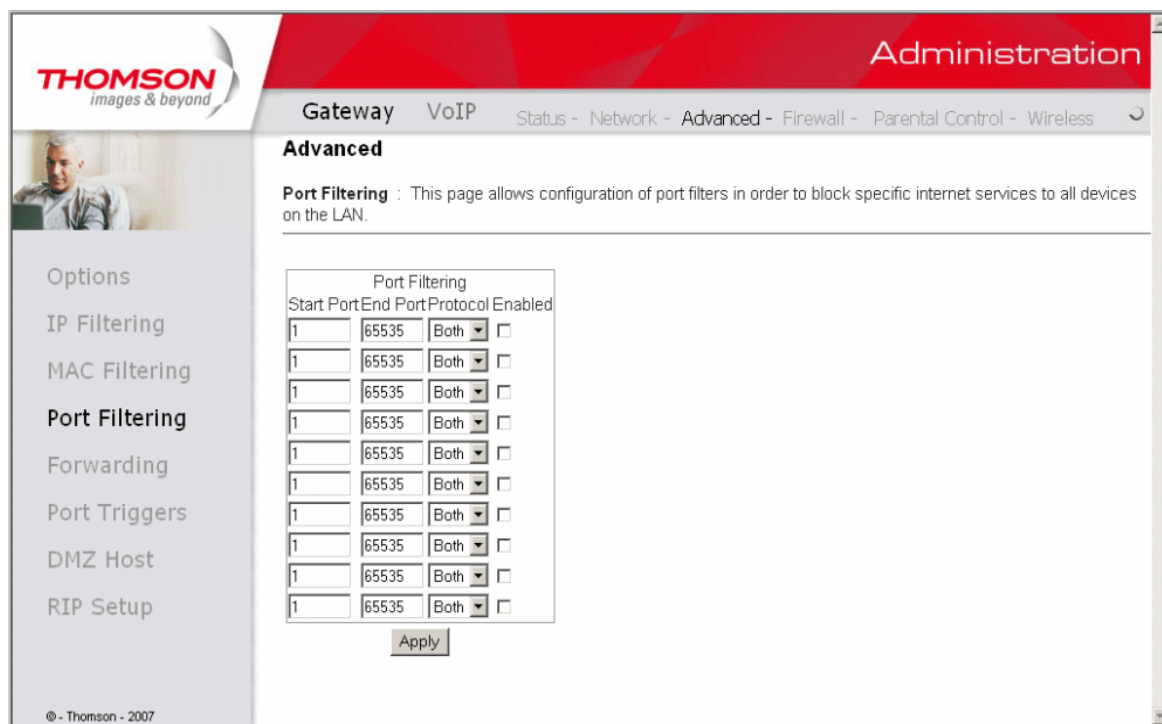
© - Thomson - 2007

Fig. 24 Gateway\Advanced\MAC Filtering

Chapter 2: WEB Configuration

4. Port Filtering

This page allows you to enter ranges of destination ports (applications) that you don't want your LAN PCs to send packets to. Any packets your LAN PCs send to these destination ports will be blocked. For example, you could block access to worldwide web browsing (http = port 80) but still allow email service (SMTP port 25 and POP-3 port 110). To enable port filtering, set Start Port and End Port for each range, and click Apply. To block only one port, set both Start and End ports with the same value.



The screenshot shows the Thomson Gateway Administration web interface. The top navigation bar includes 'Gateway', 'VoIP', and a breadcrumb trail: 'Status - Network - Advanced - Firewall - Parental Control - Wireless'. The 'Advanced' section is active, and the 'Port Filtering' page is displayed. A sidebar on the left lists various configuration options, with 'Port Filtering' selected. The main content area contains a table for configuring port filters, with columns for 'Start Port', 'End Port', 'Protocol', and 'Enabled'. The table is currently empty, and an 'Apply' button is located below it.

Start Port	End Port	Protocol	Enabled
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>

Apply

Fig. 25 Gateway\Advanced\Port Filtering

Chapter 2: WEB Configuration

5. Forwarding

For LAN ⇌ WAN communications, the gateway normally only allows you to originate an IP connection with a PC on the WAN; it will ignore attempts of the WAN PC to originate a connection onto your PC. This protects you from malicious attacks from outsiders. However, sometimes you may wish for anyone outside to be able to originate a connection to a particular PC on your LAN if the destination port (application) matches one you specify.

This page allows you to specify up to 10 such rules. For example, to specify that outsiders should have access to an FTP server you have running at 192.168.0.5, create a rule with that address and Start Port =20 and End Port =21 (FTP port ranges) and Protocol = TCP (FTP runs over TCP and the other transport protocol, UDP), and click Apply. This will cause inbound packets that match to be forwarded to that PC rather than blocked. As these connections are not tracked, no entry is made for them in the Connection Table. The same IP address can be entered multiple times with different ports.

THOMSON
images & beyond

Administration

Gateway VoIP Status - Network - Advanced - Firewall - Parental Control - Wireless

Advanced

Forwarding : This allows for incoming requests on specific port numbers to reach web servers, FTP servers, mail servers, etc. so they can be accessible from the public internet. A table of commonly used port numbers is also provided.

Local IP Addr	Start Port	End Port	Protocol	Enabled
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>

Apply

Options
IP Filtering
MAC Filtering
Port Filtering
Forwarding
Port Triggers
DMZ Host
RIP Setup

© - Thomson - 2007

Fig. 26 Gateway\Advanced\Forwarding

Chapter 2: WEB Configuration

6. Port Triggers

Some Internet activities, such as interactive gaming, require that a PC on the WAN side of your gateway be able to originate connections during the game with your game playing PC on the LAN side. You could use the Advanced-Forwarding web page to construct a forwarding rule during the game, and then remove it afterwards (to restore full protection to your LAN PC) to facilitate this. Port triggering is an elegant mechanism that does this work for you, each time you play the game.

The screenshot shows the Thomson Gateway Administration interface. The top navigation bar includes 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Advanced' section is selected, and the 'Port Triggers' sub-section is active. A sidebar on the left lists various configuration options: Options, IP Filtering, MAC Filtering, Port Filtering, Forwarding, Port Triggers (highlighted), DMZ Host, and RIP Setup. The main content area for 'Port Triggers' includes a description: 'Port Triggers : This page allows configuration of dynamic triggers to specific devices on the LAN. This allows for special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messaging program features may require these special settings.' Below this is a table for configuring triggers. The table has columns for 'Trigger Range' (Start Port, End Port), 'Target Range' (Start Port, End Port), 'Protocol', and 'Enable'. There are 10 rows, each with input fields for these values. The 'Protocol' column has a dropdown menu set to 'TCP'. An 'Apply' button is located at the bottom of the table.

Trigger Range		Target Range		Protocol	Enable
Start Port	End Port	Start Port	End Port		
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>
0	0	0	0	TCP	<input type="checkbox"/>

Apply

Fig. 27 Gateway\Advanced\Port Triggers

Port Triggering works as follows. Imagine you want to play a particular game with PCs somewhere on the Internet. You make one time effort to set up a Port Trigger for that game, by entering into **Trigger Range** the range of destination ports your game will be sending to, and entering into **Target Range** the range of destination ports the other player (on the WAN side) will be sending to (ports your PC's game receives on). Application programs like games publish this information in user manuals. Later, each time you play the game, the gateway automatically creates the forwarding rule necessary. This rule is valid until 10 minutes after it sees game activity stop. After 10 minutes, the rule becomes inactive until the next matched outgoing traffic arrives.

For example, suppose you specify Trigger Range from 6660 to 6670 and Target Range from 113 to 113. An outbound packet arrives at the gateway with your game-playing PC source IP address 192.168.0.10, destination port 666 over TCP/IP. This destination port is within the Trigger destined for port 113 to your game-playing PC at 192.168.0.10.

You can specify up to 10 port ranges on which to trigger.

Chapter 2: WEB Configuration

7. DMZ Host

Use this page to designate one PC on your LAN that should be left accessible to all PCs from the WAN side, for all ports. For example, if you put an HTTP server on this machine, anyone will be able to access that HTTP server by using your gateway IP address as the destination. A setting of “0” indicates NO DMZ PC. “Host” is another Internet term for a PC connected to the Internet.

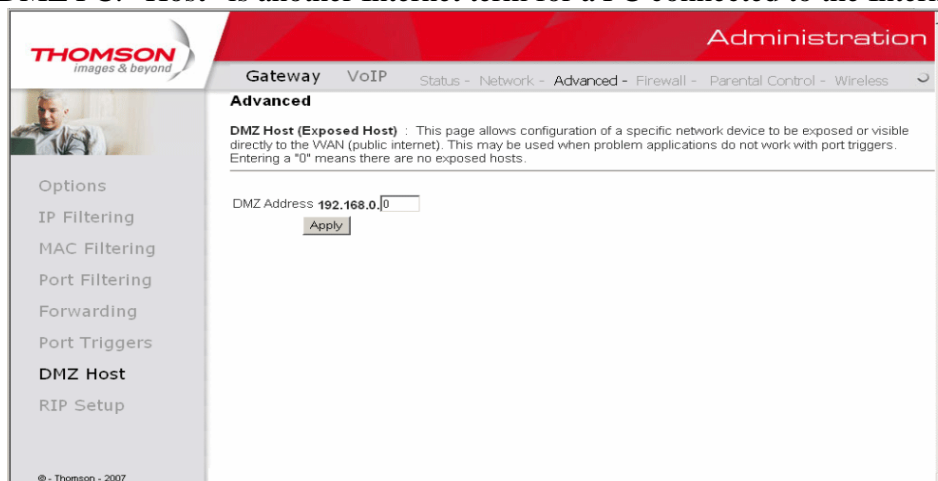


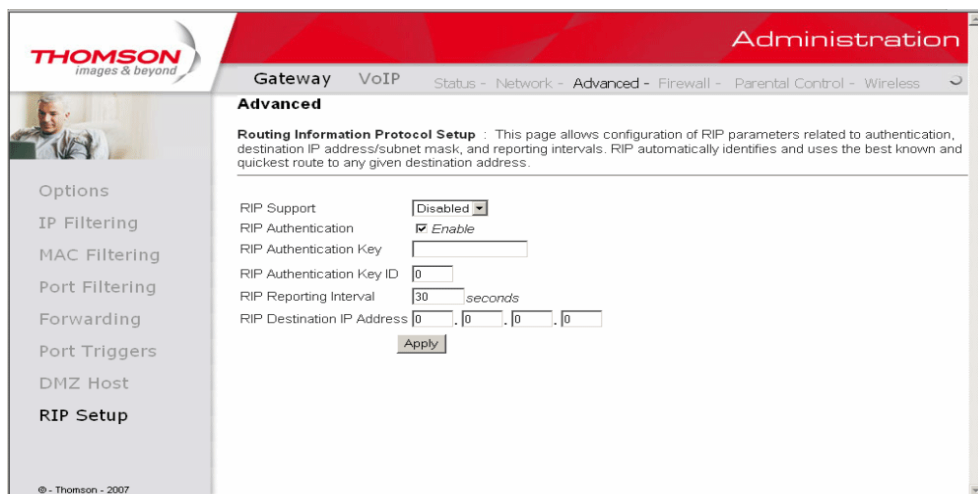
Fig. 28 Gateway\Advanced\DMZ Host

Chapter 2: WEB Configuration

8. RIP (Routing Information Protocol) Setup

This feature enables the gateway to be used in small business situations where more than one LAN (local area network) is installed. The RIP protocol provides the gateway a means to “advertise” available IP routes to these LANs to your cable operator, so packets can be routed properly in this situation.

Your cable operator will advise you during installation if any setting changes are required here.



The screenshot displays the Thomson Gateway Administration web interface. The top navigation bar includes 'Administration' and a breadcrumb trail: 'Gateway > VoIP > Status > Network > Advanced > Firewall > Parental Control > Wireless'. The left sidebar lists various configuration options, with 'RIP Setup' highlighted. The main content area is titled 'Advanced' and contains the 'Routing Information Protocol Setup' section. This section includes a descriptive paragraph and several configuration fields: 'RIP Support' (set to 'Disabled'), 'RIP Authentication' (checked 'Enable'), 'RIP Authentication Key' (empty text field), 'RIP Authentication Key ID' (set to '0'), 'RIP Reporting Interval' (set to '30' seconds), and 'RIP Destination IP Address' (four empty fields separated by dots). An 'Apply' button is located at the bottom of the configuration fields.

Fig. 29 Gateway\Advanced\RIP Setup

Chapter 2: WEB Configuration

Gateway – Firewall Web Page Group

1. Web Content Filtering

These pages allow you to enable, disable, and configure a variety of firewall features associated with web browsing, which uses the HTTP protocol and transports HTML web pages. On these pages, you designate the gateway packet types you want to have forwarded or blocked. You can activate settings by checking them and clicking Apply.

The web-related filtering features you can activate from the Web Content Filter page include Filter Proxy, Filter Cookies, Filter Java Applets, Filter ActiveX, Filter Popup Windows, and Firewall Protection.

If you want the gateway to exclude your selected filters to certain computers on your LAN, enter their MAC addresses in the Trusted Computers area of this page.

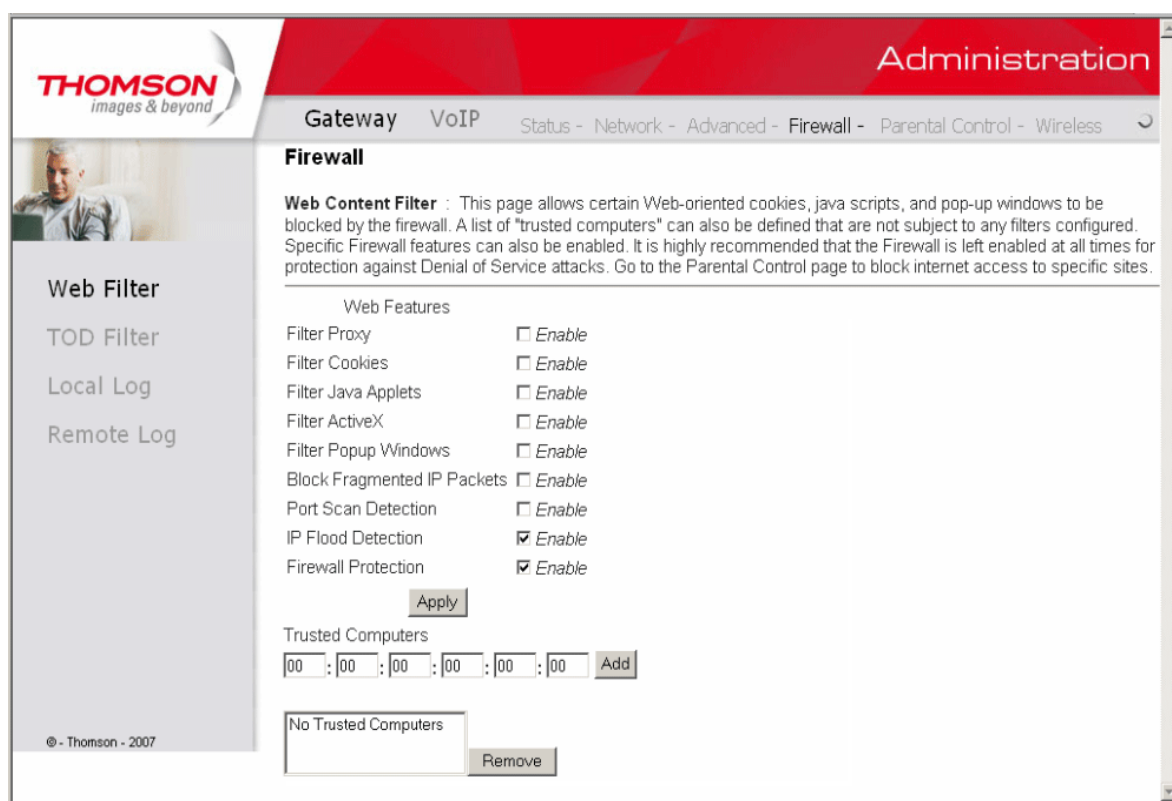


Fig. 30 Gateway\Firewall\Web Filter

Chapter 2: WEB Configuration

2. TOD Filtering

Use this page to set rules that will block specific LAN side PCs from accessing the Internet, but only at specific days and times. Specify a PC by its hardware MAC address, and then use the tools to specify blocking time. Finally, click the Apply button to save your settings.

The screenshot shows the Thomson Gateway Administration web interface. The top navigation bar includes 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Firewall' section is active, and the 'Time of Day Access Filter' page is displayed. The page title is 'Firewall'. The description states: 'Time of Day Access Filter : This page allows configuration of web access filters to block all internet traffic to and from specific network devices based on time of day settings.' The configuration area includes a MAC address input field with a placeholder '00 : 00 : 00 : 00 : 00 : 00' and an 'Add' button. Below this is a dropdown menu showing 'No filters entered.', an 'Enabled' checkbox, and a 'Remove' button. The 'Days to Block' section has checkboxes for 'Everyday', 'Sunday', 'Monday', 'Tuesday', 'Wednesday', 'Thursday', 'Friday', and 'Saturday'. The 'Time to Block' section has an 'All day' checkbox and 'Start' and 'End' time pickers, each with hour, minute, and AM/PM dropdowns. An 'Apply' button is at the bottom. The left sidebar contains links for 'Web Filter', 'TOD Filter', 'Local Log', and 'Remote Log'. The Thomson logo and 'images & beyond' tagline are in the top left. The footer shows '© - Thomson - 2007'.

Fig. 31 Gateway\Firewall\TOD Filtering

Chapter 2: WEB Configuration

3. Local Log and Remote Log

The gateway builds a log of firewall blocking actions that the firewall has taken. Using the Local Log page lets you specify an email address to which you want the gateway to email this log. You must also tell the gateway your outgoing (i.e. SMTP) email server's name, so it can direct the email to it. Enable Email Alerts has the gateway forward email notices when Firewall protection events occur. Click **E-mail Log** to immediately send the email log. Click **Clear Log** to clear the table of entries for a fresh start.

The log of these events is also visible on the screen. For each blocking event type that has taken place since the table was last cleared, the table shows Description, Count, Last Occurrence, Target, and Source.

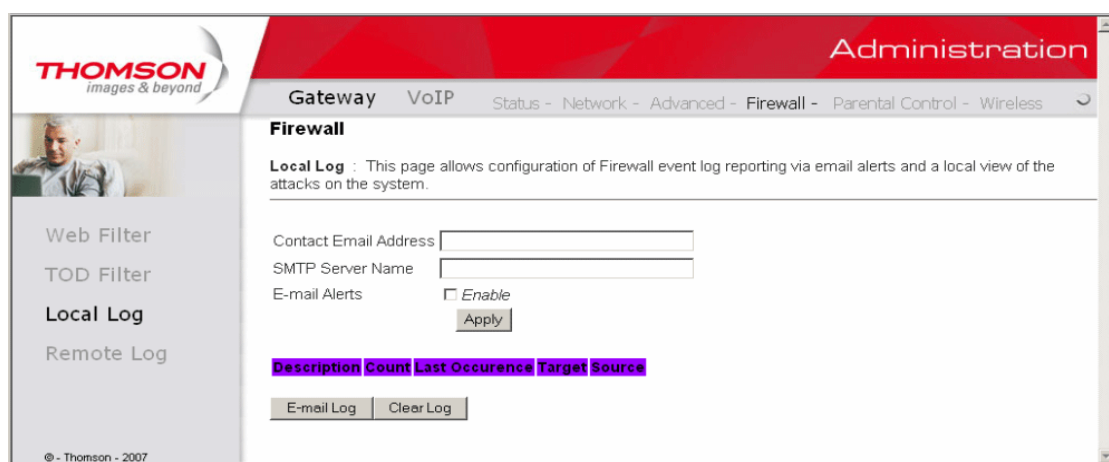


Fig. 32 Gateway\Firewall\Local Log

The Remote Log page allows you to specify the IP address where a SysLog server is located on the LAN Side and select different types of firewall events that may occur. Then, each time such an event occurs, notification is automatically sent to this log server.

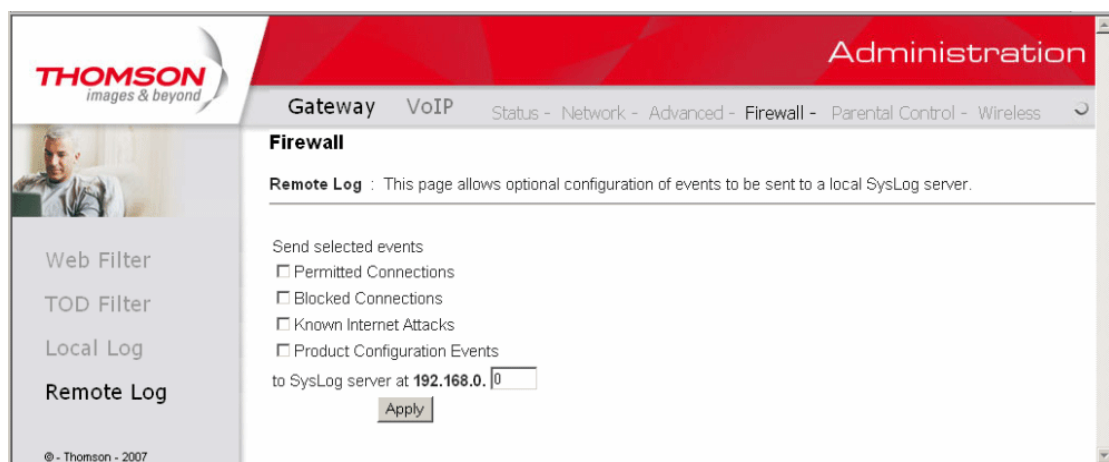


Fig. 33 Gateway\Firewall\Remote Log

Chapter 2: WEB Configuration

Gateway – Parental Control Web Page Group

1. Basic

This page allows you to enable, disable, and configure a variety of firewall features associated with web browsing, which uses the HTTP protocol and transports HTML web pages. On these pages, you designate the gateway packet types you want to have forwarded or blocked. You can activate settings by checking them and clicking Apply.

Here are some of your choices on the Parental Control page:

- Activate **Keyword Blocking** and specify some keywords in the Keyword List to cause blocking of web pages on the WAN side with the specified keyword in the content.
- Activate **Domain Blocking** and specify some Domain Names (e.g. www.ABC.com) in the Domain List.

The screenshot shows the Thomson Gateway Administration interface. The top navigation bar includes 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Parental Control' section is active, showing the 'Basic Setup' page. The page title is 'Parental Control'. The 'Basic Setup' section explains that this page allows basic selection of rules which block certain Internet content and certain Web sites. It states that when settings are changed, the 'Apply', 'Add', or 'Remove' buttons must be clicked for the settings to take effect. The 'Content Filtering' section has two options: 'Keyword Blocking' and 'Domain Blocking', both with 'Enable' checkboxes. Below these are 'Apply', 'Add Keyword', 'Remove Keyword', 'Blocked Domain List', 'Add Domain', and 'Remove Domain' buttons. The 'Keyword List' and 'Blocked Domain List' are represented by empty text boxes. The Thomson logo is in the top left corner, and the copyright notice '© - Thomson - 2007' is in the bottom left corner.

Fig. 34 Gateway\Parental Control\Basic

Chapter 2: WEB Configuration

Gateway – Wireless Web Page Group

The Wireless web pages group enables a variety of settings that can provide secure and reliable wireless communications for even the most demanding tech-savvy user.

The Wireless Voice Gateway offers a choice of 802.1x, WPA and WPA-PSK authentication of your PCs to the gateway, 64 and 128 bit WEP encryption of communication between the gateway and your PCs to guaranty security, and an Access Control List function that enables you to restrict wireless access to only your specific PCs.

Performance

Because your wireless communication travels through the air, the factory default wireless channel setting may not provide optimum performance in your home if you or your neighbors have other interfering 2.4GHz devices such as cordless phones. If your wireless PC is experiencing very sluggish or dramatically slower communication compared with the speed you achieve on your PC that is wired to the gateway, try changing the channel number. See the 802.11b/g Basic Web Page discussion below for details.

Authentication

Authentication enables you to restrict your gateway from communicating with any remote wireless PCs that aren't yours. The following minimum authentication-related changes to factory defaults are recommended. See the 802.11b/g Basic and Access Control Web Page discussions below for details.

Network Name (SSID) – Set a unique name you choose

Network Type – Set to Open

Access Control List – Enter your wireless PCs' MAC addresses

Security

Security secures or scrambles messages traveling through the air between your wireless PCs and the gateway, so they can't be observed by others. The following minimum security setting changes to factory defaults are recommended. See the 802.11b/g Security Web Page discussion below for details.

Data Encryption – Set to WPA (64-bit)

PassPhrase – Use this feature to generate security keys

Chapter 2: WEB Configuration

1. 802.11b/g/n Radio

To set the basic configuration for the wireless features, click RADIO from the Wireless menu. These must match the settings you make on your wireless-equipped PC on the LAN side.

The screenshot shows the Thomson Gateway Administration interface. At the top, a red banner reads "Please define a username and password for administration" and "Click here to change the settings". The "Administration" title is on the right. Below the banner is a navigation bar with tabs: Gateway, VoIP, Status, Network, Advanced, Firewall, Parental Control, and Wireless. The "Wireless" tab is selected. On the left is a sidebar menu with options: Radio, Primary Network, Guest Network, Access Control, Advanced, Bridging, and WMM. The "Radio" option is selected. The main content area is titled "Wireless" and contains a description: "802.11 Radio : This page allows configuration of the Wireless Radio including current country and channel number." Below this is a form with the following fields and values: Interface (Enabled), Wireless MAC Address (00:26:24:1c:98:6e), Output Power (100%), 802.11 Band (2.4 Ghz), 802.11 n-mode (Auto), Bandwidth (20 Mhz), Sideband for Control Channel (40 Mhz only) (Lower), Control Channel (7), and Current Channel (7). At the bottom of the form are two buttons: "Apply" and "Restore Wireless Defaults". The Thomson logo and "© - Thomson - 2007" are in the bottom left corner.

Fig. 35 Gateway\Wireless\Radio

- **Interface:** The wireless radio in your gateway can be completely de-activated by changing **Interface** to Disabled. Click the **Apply** button to save your settings. Activated by changing interface to enabled.
- **Wireless MAC Address:** The MAC address for this wireless device will be displayed in this field automatically.
- **Output Power:**
This setting decides the output power of this device. You may use it to economize on electricity by selecting lower percentage of power output. Control the range of the AP by adjusting the radio output power.
- **802.11 Band:** It can Support 2.4 GHz and 5 GHz exclusively.
- **802.11n mode:** It may help you to **Enable** or **Disable** the 11N mode. To enable you need to select **Auto**, to disable you need to select **Off**, and so force the AP to operate in 802.11g mode.
- **Bandwidth:** Select wireless channel width 20Mhz is for default value (bandwidth taken by

Chapter 2: WEB Configuration

wireless signals of this access point.)

- **Sideband for Control Channel (40Mhz only):** There are “Lower” and “Upper” can be selected if Bandwidth 40Mhz is Enabled.
- **Control Channel:** There are 13 channels that you can choose. Choose the one that is suitable for this device.
- **Current Channel:** The channel that you choose will be displayed in this field.
- **Restore Wireless defaults:** To recover to the default settings, press this button to retrieve the settings and click Apply.

Setting	Description	Value List or Range	Default
Network Name (SSID)	Set the Network Name (also known as SSID) of this network.	Up to 32-character string containing ASCII characters only	THOM_Dxxxxxxx
Network Type	Select Closed to hide the network from active scans. Select Open to reveal the network to active scans.	Open, Closed	Open
New Channel	Select a particular channel on which to operate.	1-13	1, 6 or 11
Interface	Enable or disable the wireless interface.	Enabled, Disabled	Enabled

Table1. Basic Settings Definitions

Chapter 2: WEB Configuration

2. 802.11b/g/n Primary Network

This page allows you to configure the Network Authentication. It provides several different modes of wireless security. You will have to enter proper information according to the mode you select.

The screenshot shows the Thomson Gateway Administration interface. The top navigation bar includes 'Gateway', 'VoIP', 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', and 'Wireless'. The 'Wireless' section is active, showing the '802.11 Primary Network' configuration page. The page title is '802.11 Primary Network : This page allows configuration of the Primary Wireless Network and its security settings.' The configuration fields are as follows:

- Primary Network Thom_D2046917 (00:26:24:1c:98:6e)
- Primary Network: Enabled (dropdown)
- Automatic Security Configuration: Disabled (dropdown)
- Network Name (SSID): Thom_D2046917
- Closed Network: Open (dropdown)
- WPA: Disabled (dropdown)
- WPA-PSK: Enabled (dropdown)
- WPA2: Disabled (dropdown)
- WPA2-PSK: Enabled (dropdown)
- WPA/WPA2 Encryption: TKIP+AES (dropdown)
- WPA Pre-Shared Key: [Redacted]
- Show Key: ☐
- RADIUS Server: 0.0.0.0
- RADIUS Port: 1812
- RADIUS Key: [Redacted]
- Group Key Rotation Interval: 0
- WPA/WPA2 Re-auth Interval: 3600
- WEP Encryption: Disabled (dropdown)
- Shared Key Authentication: Optional (dropdown)
- 802.1x Authentication: Disabled (dropdown)
- Network Key 1: [Redacted]
- Network Key 2: [Redacted]
- Network Key 3: [Redacted]
- Network Key 4: [Redacted]
- Current Network Key: 1 (dropdown)
- PassPhrase: [Redacted]
- Generate WEP Keys: [Button]
- Apply: [Button]

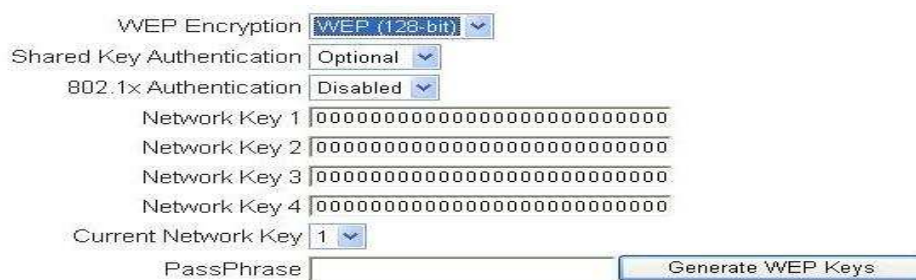
Fig. 36 Gateway\Primary Network

- **WPA (Wi-Fi Protected Access)/WPA2:**

It must be used in conjunction with an authentication server such as RADIUS to provide centralized access control and management. It can provide stronger encryption and authentication solution than none WPA modes. **WPA2** is the second generation of **WPA** security

Chapter 2: WEB Configuration

- **WPA-PSK (WPA-Pre-Shared Key) /WPA2-PSK (WPA2-Pre-Shared Key):**
It is useful for small places without authentication servers such as the network at home. It allows the use of manually-entered keys or passwords and is designed to be easily set up for home users.
- **WEP Encryption:**
You can choose **64-bit** or **128-bit** according to your needs. If you choose **Disabled**, the Network Keys will not be shown on this page. If selected, the data is encrypted using the key before being transmitted. For example, if you set 128-bit in this field, then the receiving station must be set to use the 128 Bit Encryption, and have the same Key value too. Otherwise, it will not be able to decrypt the data.
(Note: You need to connect one end of the Ethernet cable to the Ethernet port on the back of your computer, and the other end to the ETHERNET port on the Wireless Voice Gateway.)
- If you select WEP (**64-bit** or **128-bit**), you can adjust the following settings-
- **Shared Key Authentication:** Decide whether to set the shared key **Optional** or **Required** by selecting from the drop-down menu.
- **Network Key 1 to 4:** The system allows you to enter four sets of the WEP key. For **64-bit** WEP mode, the key length is 5 characters or 10 hexadecimal digits. As for **128-bit** WEP mode, the key length is 13 characters or 26 hexadecimal digits.
- **Current Network Key:** Select one set of the network key (from 1 to 4) as the default one.
- **PassPhrase:** You can enter ASCII codes into this field. The range is from 8 characters to 64 characters. For **ASCII characters**, you can key in **63** characters in this field. If you want to key in **64** characters, only **hexadecimal characters** can be used.
- **Generate WEP Keys:** Click this button to generate the PassPhrase.



The screenshot displays a web configuration page for WEP encryption. At the top, 'WEP Encryption' is set to 'WEP (128-bit)' via a dropdown menu. Below it, 'Shared Key Authentication' is set to 'Optional' and '802.1x Authentication' is set to 'Disabled'. There are four rows for 'Network Key 1' through 'Network Key 4', each with a text input field containing 26 zeros. Below these is a 'Current Network Key' dropdown menu set to '1'. At the bottom, there is a 'PassPhrase' text input field and a 'Generate WEP Keys' button.

Fig. 37 PassPhrase

- **Apply:** After proper configuration, click Apply to invoke the settings.

Chapter 2: WEB Configuration

802.1x Authentication

If you enable the **802.1x authentication** function, you will have to offer the following information-

- **RADIUS Server:** RADIUS Server is a protocol for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server. Please key in the IP Address for the RADIUS Server.
- **RADIUS Port:** Besides the IP address of the RADIUS Server, you have to enter the port number for the server. Port 1812 is the reserved RADIUS-authentication port described in RFC 2138. Earlier AP (RADIUS clients) use port 1945. The default value will be shown on this box. You can keep and use it.
- **RADIUS Key:** A RADIUS Key is like a password, which is used between IAS and the specific RADIUS client to verify identity. Both IAS and the RADIUS client must be use the same RADIUS Key for successful communication to occur. Enter the RADIUS Key.

WPA/WPA2 Encryption

WPA Pre-Shared Key

RADIUS Server

RADIUS Port

RADIUS Key

Group Key Rotation Interval

WPA/WPA2 Re-auth Interval

WEP Encryption

Shared Key Authentication

802.1x Authentication

Network Key 1

Network Key 2

Network Key 3

Network Key 4

Current Network Key

PassPhrase

Fig. 38 802.1x Authentication

Chapter 2: WEB Configuration

WPA/WPA2

For the WPA/WPA2 network Authentication, the settings that you can adjust including WPA/WPA2 Encryption, RADIUS Server, RADIUS Port, RADIUS Key, Group Key Rotation Interval, and WPA/WPA2 Re-auth Interval.

- **WPA/WPA2 Encryption:** There are three types that you can choose, **TKIP***, **AES****, **TKIP+AES**.

TKIP takes the original master key only as a starting point and derives its encryption keys mathematically from this mater key. Then it regularly changes and rotates the encryption keys so that the same encryption key will never be used twice

**** AES** provides security between client workstations operating in ad hoc mode. It uses a mathematical ciphering algorithm that employs variable key sizes of 128, 192 or 256 bits.

- **RADIUS Server/RADIUS Port/RADIUS Key:** Please refer to the previous page.
- **Group Key Rotation Interval:** Key in the time for the WAP group key rotation interval. The unit is second. With increasing rekey interval, user bandwidth requirement is reduced.
- **WPA/WPA2 Re-auth Interval:** When a wireless client has associated with the Wireless Voice Gateway for a period of time longer than the setting here, it would be disconnected and the authentication will be executed again. The default value is 3600, you may modify it.

The image shows a web configuration interface for WPA/WPA2 settings. It includes several dropdown menus and text input fields. The settings are as follows:

Setting	Value
WPA	Enabled
WPA-PSK	Disabled
WPA2	Disabled
WPA2-PSK	Disabled
WPA/WPA2 Encryption	TKIP
WPA Pre-Shared Key	[Empty field]
RADIUS Server	0.0.0.0
RADIUS Port	1812
RADIUS Key	[Empty field]
Group Key Rotation Interval	0
WPA/WPA2 Re-auth Interval	3600

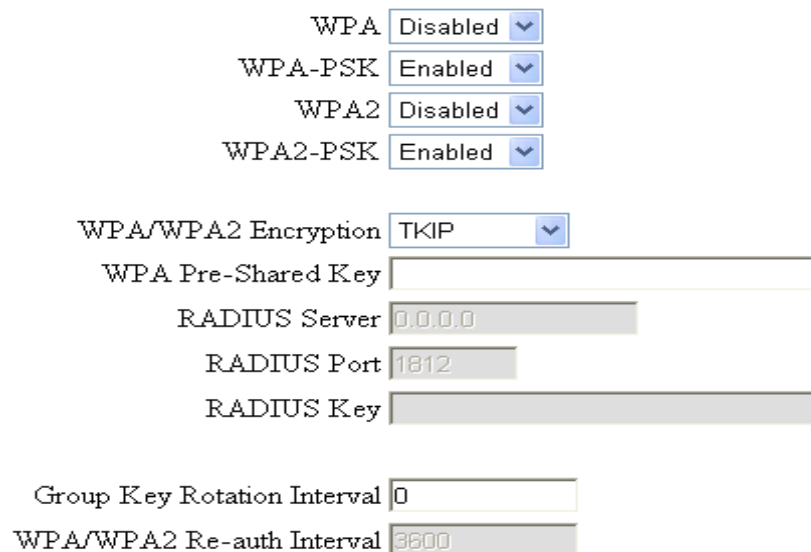
Fig. 39 WPA/WPA2

Chapter 2: WEB Configuration

WPA-PSK/ WPA2-PSK

For the WPA-PSK/WPA2-PSK network Authentication, the settings that you can adjust including WPA/WPA2 Encryption, WPA Pre-Shared Key, and Group key Rotation Interval.

- **WPA Pre-Shared Key:** Please type the key to be between 8 and 63 characters, or 64 hexadecimal digits. Only the devices with a matching key that you set here can join this network.
- WPA/WPA2 Encryption & WPA Group Rekey Interval : **Please refer to the WPA/WPA2 part.**



The image shows a configuration interface for WPA-PSK/WPA2-PSK. It includes several dropdown menus and text input fields. The 'WPA' dropdown is set to 'Disabled', 'WPA-PSK' is 'Enabled', 'WPA2' is 'Disabled', and 'WPA2-PSK' is 'Enabled'. The 'WPA/WPA2 Encryption' dropdown is set to 'TKIP'. The 'WPA Pre-Shared Key' field is empty. The 'RADIUS Server' field contains '0.0.0.0', 'RADIUS Port' contains '1812', and 'RADIUS Key' is empty. The 'Group Key Rotation Interval' field contains '0', and 'WPA/WPA2 Re-auth Interval' contains '3600'.

WPA	Disabled
WPA-PSK	Enabled
WPA2	Disabled
WPA2-PSK	Enabled
WPA/WPA2 Encryption	TKIP
WPA Pre-Shared Key	
RADIUS Server	0.0.0.0
RADIUS Port	1812
RADIUS Key	
Group Key Rotation Interval	0
WPA/WPA2 Re-auth Interval	3600

Fig. 40 WPA-PSK/WPA2-PSK

Chapter 2: WEB Configuration

Automatic Security Configuration

WPS ▼

WPS Config State: Unconfigured

The physical button on the AP will provision wireless clients using Wi-Fi Protected Setup (WPS)

Device Name: ThomsonAP

WPS Setup AP

PIN: 12345670

WPS Add Client

Add a client: ☐ Push-Button ☒ PIN

PIN:

Fig. 41 Automatic Security Configuration

WiFi Protected Setup (WPS) is an easy and secure way of configuring and connecting your WiFi access point. In your case, the TWG870 is the Access Point (AP), and Your PC (or Wifi Device) is called the STA. When configuring your Wifi Network via WPS, Messages are exchanged between the STA and AP in order to configure the Security Settings on both devices.

- **WPS Config:** It will help you to **Enable** or **Disable** the WPS feature. To enable you need to select **WPS**, to disable you need to select **Disabled**.

Note: After you **Enabled** the WPS you will get the options as show in Fig.35 and the WPS Config State box will show its configuration status.

- **Device Name:** By using this you can change the factory default to a name of your choice which is up to 32 characters long as like **SSID**.
- **WPS Setup AP:** Here you do not need to change anything, just skip this step.
- **WPS Add Client:** There are two methods “Push-Button” and “PIN”. Select the method you want.
But, the default selection will be “PIN”.

Chapter 2: WEB Configuration

If you select “Push-Button”, then the **WPS Add Client** option will appear as shown below.

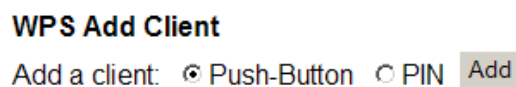


Fig. 42 WPS/Push-Button

And then if you click “Add” button then **WPS Setup AP** page will appear as shown in Fig.38

WPS Setup AP

Your AP is now waiting for the STA to connect.

PUSH

WPS Configure Status: InProgress

Fig. 43 WPS Setup AP/PUSH

And **WPS Configure Status** will be “In progress”, after establishing the connection the **WPS Configure Status** will be “Success!” as shown below. After successful connection the client will get IP address from AP and then internet will be accessible.

WPS Setup AP SUCCESSFUL

AP Configuration is complete. Click 'Continue' to return to the previous page.

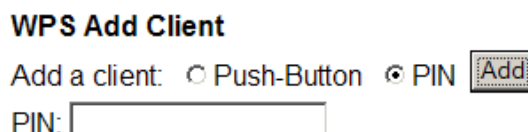
Continue

WPS Configure Status: Success!

Fig. 44 WPS Setup AP successful/PUSH

Chapter 2: WEB Configuration

If you select **WPS Method** to PIN then it will ask for PIN while configuring the WiFi AP by showing a text box so, you need to enter PIN to establish the connection. You can get the PIN from your connected Wi-Fi client.



WPS Add Client

Add a client: ☐ Push-Button ☒ PIN

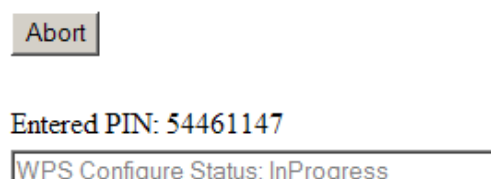
PIN:

Fig. 45 WPS/PIN

- **PIN:** Use this option to set the PIN, enter 4-8 digits PIN of the device you wish to configure. After entering the pin click “Add” button, then the WPS Setup AP page will appear as shown in Fig.41

WPS Setup AP

Your AP is now waiting for the STA to connect.



Entered PIN: 54461147

WPS Configure Status: InProgress

Fig. 46 WPS Setup AP/PIN

And **WPS Configure Status** will be “In progress”, after establishing the connection the **WPS Configure Status** will be “Success!” as shown below. After successful connection the client will get IP address from AP and then internet will be accessible.

Chapter 2: WEB Configuration

WPS Setup AP SUCCESSFUL

AP Configuration is complete. Click 'Continue' to return to the previous page.

Continue

Entered PIN:

WPS Configure Status: Success!

Fig. 47 WPS Setup AP successful/PIN

Chapter 2: WEB Configuration

3. Guest Network

This page allows you to configure a guest network.

You can refer to the details described in previous sections to make the WiFi security settings and guest LAN settings.

A Guest Network is a Wireless Network independent from the Main Wireless Network (also called “Primary Network”). It can be setup to have 2 different Wireless Network: one for you and your family, and one for your guests. Security settings for the 2 Networks can be different.

Note: that this functionality may be disabled by your Cable Operator.

Chapter 2: WEB Configuration

The screenshot shows the Thomson Gateway Administration interface. The top navigation bar includes links for Gateway, VoIP, Status, Network, Advanced, Firewall, Parental Control, and Wireless. The 'Wireless' section is active, showing the '802.11 Guest Network' configuration page. The page is divided into two main sections: 'Guest WiFi Security Settings' and 'Guest LAN Settings'. The 'Guest WiFi Security Settings' section includes fields for Guest Network Name (SSID), Closed Network, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA/WPA2 Encryption, WPA Pre-Shared Key, RADIUS Server, RADIUS Port, RADIUS Key, Group Key Rotation Interval, and WPA/WPA2 Re-auth Interval. The 'Guest LAN Settings' section includes fields for DHCP Server, IP Address, Subnet Mask, Lease Pool Start, Lease Pool End, and Lease Time. There are buttons for 'Apply', 'Restore Guest Network Defaults', and 'Generate WEP Keys'.

THOMSON
images & beyond

Please define a username and password for administration
Click [here](#) to change the settings

Administration

Gateway VoIP Status - Network - Advanced - Firewall - Parental Control - Wireless

Wireless

802.11 Guest Network : This page allows configuration of a guest network.

Guest Network Thom_G2631020 (02:26:24:1c:98:6f)

Guest WiFi Security Settings

Guest Network Enabled

Guest Network Name (SSID) Thom_G2631020

Closed Network Open

WPA Disabled

WPA-PSK Enabled

WPA2 Disabled

WPA2-PSK Disabled

WPA/WPA2 Encryption AES

WPA Pre-Shared Key

☐ Show Key

RADIUS Server 0.0.0.0

RADIUS Port 1812

RADIUS Key

Group Key Rotation Interval 0

WPA/WPA2 Re-auth Interval 3600

Guest LAN Settings

DHCP Server Disabled

IP Address 192.168.1.1

Subnet Mask 255.255.255.0

Lease Pool Start 192.168.1.10

Lease Pool End 192.168.1.99

Lease Time 86400

Apply

Restore Guest Network Defaults

WEP Encryption Disabled

Shared Key Authentication Optional

802.1x Authentication Disabled

Network Key 1

Network Key 2

Network Key 3

Network Key 4

Current Network Key 2

PassPhrase

Generate WEP Keys

Apply

© - Thomson - 2007

Fig.48 Gateway\Wireless\Guest Network

Chapter 2: WEB Configuration

4. Access Control

This page allows you to make access control to the AP or connected clients by offering the MAC Addresses of the clients.

Fig. 49 Gateway\Wireless\Access Control

- **Administration Web Page Access :** Select **Allow** to permit access to Administration Web Page from PC connected over Wifi; or choose **Deny** to prevent the clients connected over Wifi from access to Administration Web Page.
- **MAC Restrict Mode :** Click **Disabled** to welcome all of the clients on the network; select **Allow** to permit only the clients on the list to access the cable modem; or choose **Deny** to prevent the clients on the list to access this device.
- **MAC Address :** Your Gateway identifies wireless PCs by their WiFi MAC Address. This address consists of a string of 6 pairs of numbers 0-9 and letters A-F, such as 00 90 4B F0 FF 50. It is usually printed on the WiFi card of the device (e.g. the PCMCIA card in a laptop).
- Enter the MAC addresses of the connected clients into the fields, and then click Apply to add them to the list for access control.
- **Apply :** After proper configuration, click Apply to invoke the settings.
- **Connected Clients :** The information of currently connected clients will be displayed here.

Chapter 2: WEB Configuration

5. 802.11Advanced

This page allows you to configure some advanced settings. The factory default values should provide good results in most cases. We don't recommend you change these settings unless you have technical knowledge of 802.11b wireless technology.

For expert users, details of all settings on this web page are provided below.

THOMSON
images & beyond

Please define a username and password for administration
Click [here](#) to change the settings

Administration

Gateway VoIP Status - Network - Advanced - Firewall - Parental Control - Wireless

Wireless

802.11 Advanced : This page allows configuration of data rates and WiFi thresholds.

54g™ Mode 54g Auto

Basic Rate Set Default

54g™ Protection Auto

XPress™ Technology Disabled

Afterburner™ Technology Disabled

Rate Auto

Beacon Interval 100

DTIM Interval 1

Fragmentation Threshold 2346

RTS Threshold 2347

NPHY Rate Auto

802.11n Protection Auto

Multicast Rate Auto

Apply

© - Thomson - 2007

Fig. 50 Gateway\Wireless\Advanced

- **Beacon Interval:**
Set the period of beacon transmissions to allow mobile stations to locate and identify a BSS. The measure unit is “time units” (TU) of 1024 microseconds. (Value range: 1~65535)
- **DTIM Interval:**
The value you set here is used to inform mobile stations when multicast frames that have been buffered at the Wireless Voice Gateway will be delivered and how often that delivery occurs. (Value range: 1~255)
- **Fragmentation Threshold:**
Set the number of the fragmenting frames to make the data to be delivered without errors induced by the interference. Frames longer than the value you set here are fragmented before the initial transmission into fragments no longer than the value of the threshold. (Value range: 256~ 2346)
- **RTS Threshold:**

Chapter 2: WEB Configuration

Set the value for sending a request to the destination. All the frames of a length greater than the threshold that you set here will be sent with the four-way frame exchange. And, a length less than or equal to the value that you set will not be proceeded by RTS. (Value range: 0~ 2347)

- **54gTM Network Mode:**

There are three modes for you to choose, please check the specification of your wireless card and choose a proper setting.

- **54gTM Protection:**

Select **Auto** to turn on the 54gTM protection; select **Off** to turn down the protection.

- **XpressTM Technology:**

When Xpress is turned on, aggregate throughput (the sum of the individual throughput speeds of each client on the network) can improve by **up to** 27% in 802.11g-only networks, and **up to** 75% in mixed networks comprised of 802.11g and 802.11b standard equipment.

- **Rate:**

It decides the speed of data transmission. There are several rates provided here for you to choose. Choose any one of it according to your needs by using the drop-down menu.

- **Output Power:**

To reduce the output power.

Chapter 2: WEB Configuration

6. Bridging

The Bridging page provides a location where settings can be adjusted related to the WDS (**Wireless Distribution System**) feature.

WDS is a system that enables the interconnection of access points wirelessly. It may also be referred to as repeater mode because it appears to bridge and accept wireless clients at the same time (unlike traditional bridging).

The wireless gateway can be placed in a mode that allows the gateway to communicate with other “extender” wireless access points either exclusively or mixed with communications to local PCs. Use this page to designate the Remote Bridges the gateway is allowed to communicate with, and to select the Wireless Bridging mode.

The screenshot shows the Thomson Gateway Administration interface. At the top, a red banner reads "Please define a username and password for administration" and "Click [here](#) to change the settings". The "Administration" title is on the right. Below the banner, a navigation bar includes "Gateway", "VoIP", "Status", "Network", "Advanced", "Firewall", "Parental Control", and "Wireless". The "Wireless" tab is selected. On the left, a sidebar menu lists "Radio", "Primary Network", "Guest Network", "Access Control", "Advanced", "Bridging" (highlighted), and "WMM". The main content area is titled "Wireless" and contains a "Bridging" section with the text "This page allows configuration of WDS features." Below this, there is a "Wireless Bridging" dropdown menu set to "Disabled", followed by four empty text boxes for "Remote Bridges", and an "Apply" button at the bottom. The Thomson logo and "© - Thomson - 2007" are visible in the bottom left corner.

Fig. 51 Gateway\Wireless\Bridging

- **Wireless Bridging:**
Choose **Disabled** to shutdown this function; select **Enabled** to turn on the function of WDS.
- **Remote Bridges:**
Enter the MAC Addresses of the remote Bridges to relay the signals for each other.
- **Apply:**
After proper configuration, click Apply to invoke the settings.

Chapter 2: WEB Configuration

7. 802.11e QoS (WMM) Settings

Wi-Fi Multimedia (WMM) is a component of the IEEE 802.11e wireless LAN standard for quality of service (QoS). The QoS assigns priority to the selected network traffic and prevents packet collisions and delays thus improving VoIP calls and watching video over WLANs.

- **Enable WMM:**

This field allows you to enable WMM to improve multimedia transmission.

- **Enable WMM No-Acknowledgement:**

This field allows you to enable WMM No-Acknowledgement.

- **Power Save Support:**

This field allows you to enable WMM Power-Save-Support.

The screenshot shows the Thomson Gateway Administration interface. The top navigation bar includes links for Gateway, VoIP, Status, Network, Advanced, Firewall, Parental Control, and Wireless. The 'Wireless' tab is selected. Below the navigation bar, the '802.11 Wi-Fi Multimedia' section is active, displaying configuration options for WMM Support, No-Acknowledgement, and Power Save Support. The 'EDCA AP Parameters' table is also visible, showing settings for AC_BE, AC_BK, AC_VI, and AC_VO. The 'EDCA STA Parameters' table is also present, showing settings for AC_BE, AC_BK, AC_VI, and AC_VO. The 'Apply' button is located at the bottom of the configuration area.

WMM Support **No-Acknowledgement** **Power Save Support**

EDCA AP Parameters:	CWmin	CWmax	AIFSN	TXOP(b) Limit (usec)	TXOP(a/g) Limit (usec)	Discard Oldest First
AC_BE	15	63	3	0	0	<input type="button" value="Off"/>
AC_BK	15	1023	7	0	0	<input type="button" value="Off"/>
AC_VI	7	15	1	6016	3008	<input type="button" value="Off"/>
AC_VO	3	7	1	3264	1504	<input type="button" value="Off"/>

EDCA STA Parameters:

AC_BE	15	1023	3	0	0
AC_BK	15	1023	7	0	0
AC_VI	7	15	2	6016	3008
AC_VO	3	7	2	3264	1504

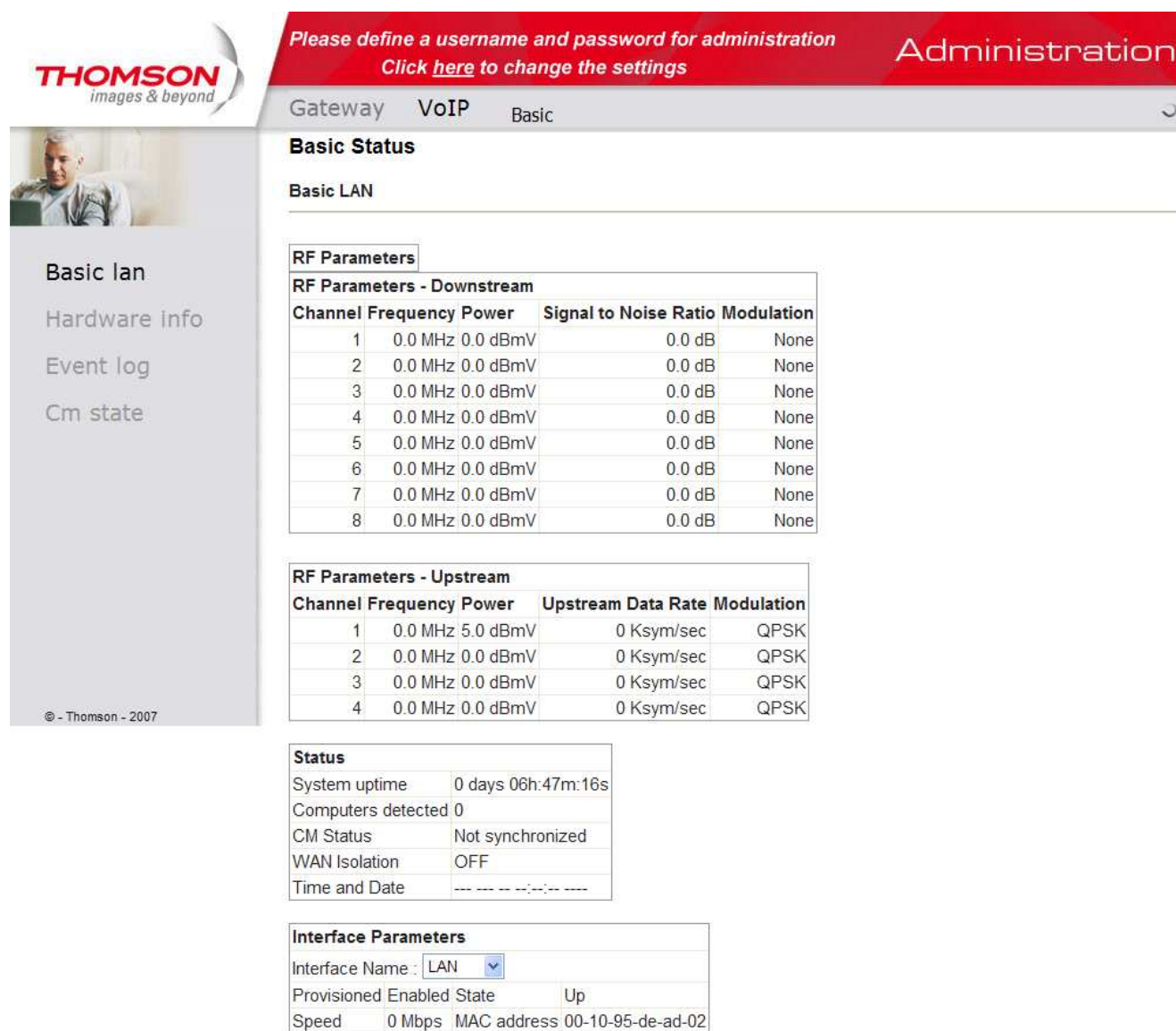
Fig. 52 Gateway\Wireless\WMM

Chapter 2: WEB Configuration

VoIP – Basic Web Page Group

1. Basic LAN

This page displays the basic LAN status of this device, including the downstream and upstream status, device information, and interface parameters. You can select specific interface from the Interface Name drop-down menu.



THOMSON
images & beyond

Please define a username and password for administration
Click [here](#) to change the settings

Administration

Gateway VoIP Basic

Basic Status

Basic LAN

RF Parameters

RF Parameters - Downstream

Channel	Frequency	Power	Signal to Noise Ratio	Modulation
1	0.0 MHz	0.0 dBmV	0.0 dB	None
2	0.0 MHz	0.0 dBmV	0.0 dB	None
3	0.0 MHz	0.0 dBmV	0.0 dB	None
4	0.0 MHz	0.0 dBmV	0.0 dB	None
5	0.0 MHz	0.0 dBmV	0.0 dB	None
6	0.0 MHz	0.0 dBmV	0.0 dB	None
7	0.0 MHz	0.0 dBmV	0.0 dB	None
8	0.0 MHz	0.0 dBmV	0.0 dB	None

RF Parameters - Upstream

Channel	Frequency	Power	Upstream Data Rate	Modulation
1	0.0 MHz	5.0 dBmV	0 Ksym/sec	QPSK
2	0.0 MHz	0.0 dBmV	0 Ksym/sec	QPSK
3	0.0 MHz	0.0 dBmV	0 Ksym/sec	QPSK
4	0.0 MHz	0.0 dBmV	0 Ksym/sec	QPSK

Status

System uptime	0 days 06h:47m:16s
Computers detected	0
CM Status	Not synchronized
WAN Isolation	OFF
Time and Date	---

Interface Parameters

Interface Name :	LAN		
Provisioned	Enabled	State	Up
Speed	0 Mbps	MAC address	00-10-95-de-ad-02

© - Thomson - 2007

Fig. 53 VoIP\Basic\Basic LAN

Chapter 2: WEB Configuration

2. Hardware Info

The hardware Info is displayed on this page.

The screenshot shows the Thomson VoIP Basic web configuration interface. At the top, a red banner contains the text "Please define a username and password for administration" and "Click [here](#) to change the settings". The word "Administration" is displayed in the top right corner. Below the banner, a navigation bar shows "Gateway", "VoIP", and "Basic" tabs, with "Basic" being the active tab. On the left side, there is a sidebar with the Thomson logo and a list of menu items: "Basic lan", "Hardware info" (which is highlighted), "Event log", and "Cm state". The main content area is titled "Basic Status" and "Hardware Info". It contains three sections: "System" with a table of hardware and software details, "MTA Hardware Information" with the Mta Serial Number, and "Software Build and Revisions" with the Firmware Name and Build Time.

System			
HW Revision	1.0	VENDOR	Thomson
BOOT Revision	2.3.0	SW Revision	STB2.01.12.T2
MODEL	TWG870U	Software Version	STB2.01.12.T2
Serial Number	54321740512349		

MTA Hardware Information	
Mta Serial Number	54321740512349

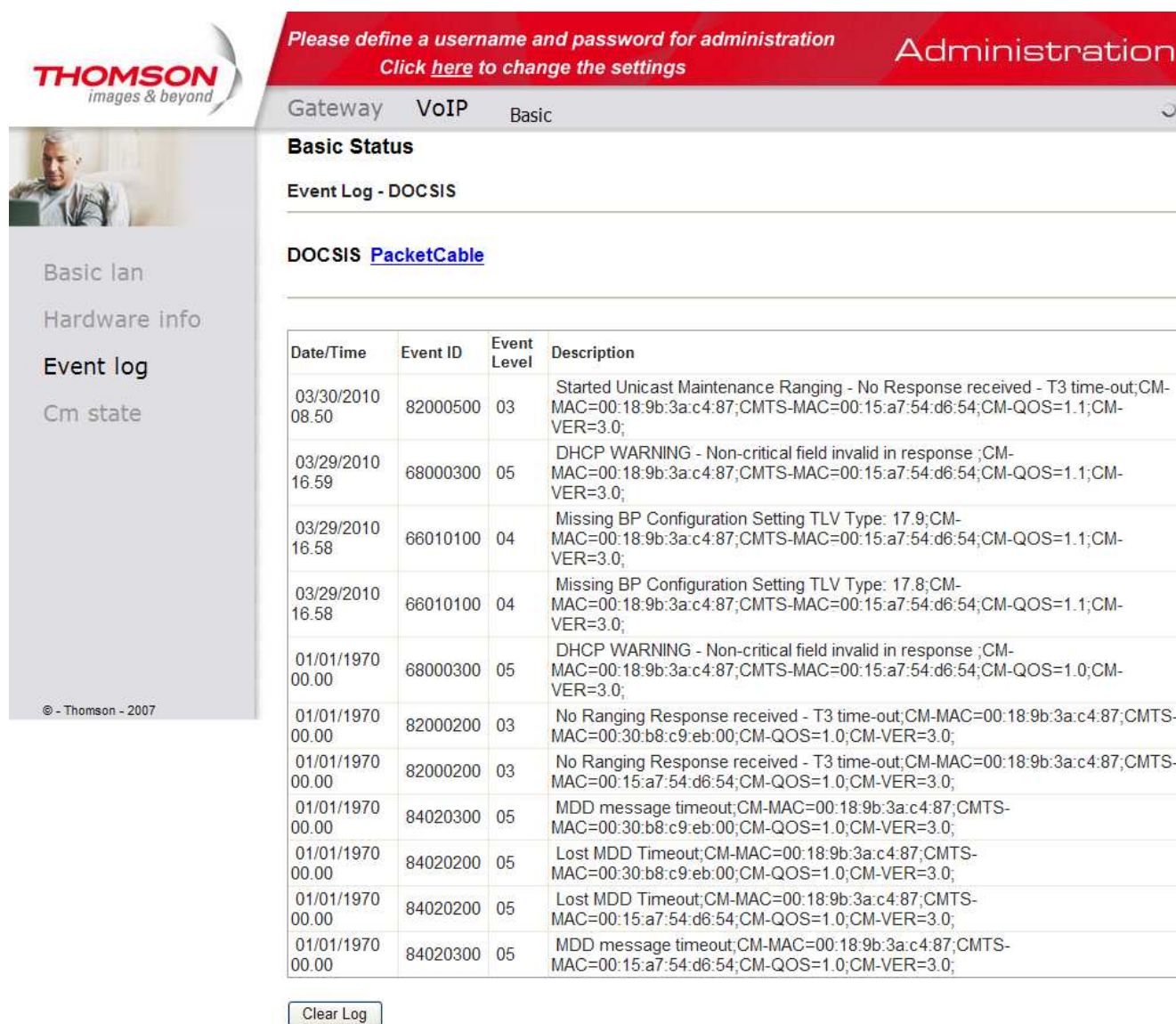
Software Build and Revisions	
Firmware Name	TWG870-B2.01.12.T2-100324-F-1C1.bin
Firmware Build Time	15:32:55 Wed Mar 24 2010

Fig. 54 VoIP\Basic\Hardware Info

Chapter 2: WEB Configuration

3. Event Log

The event logs are displayed on this web page. You can check them whenever you need.



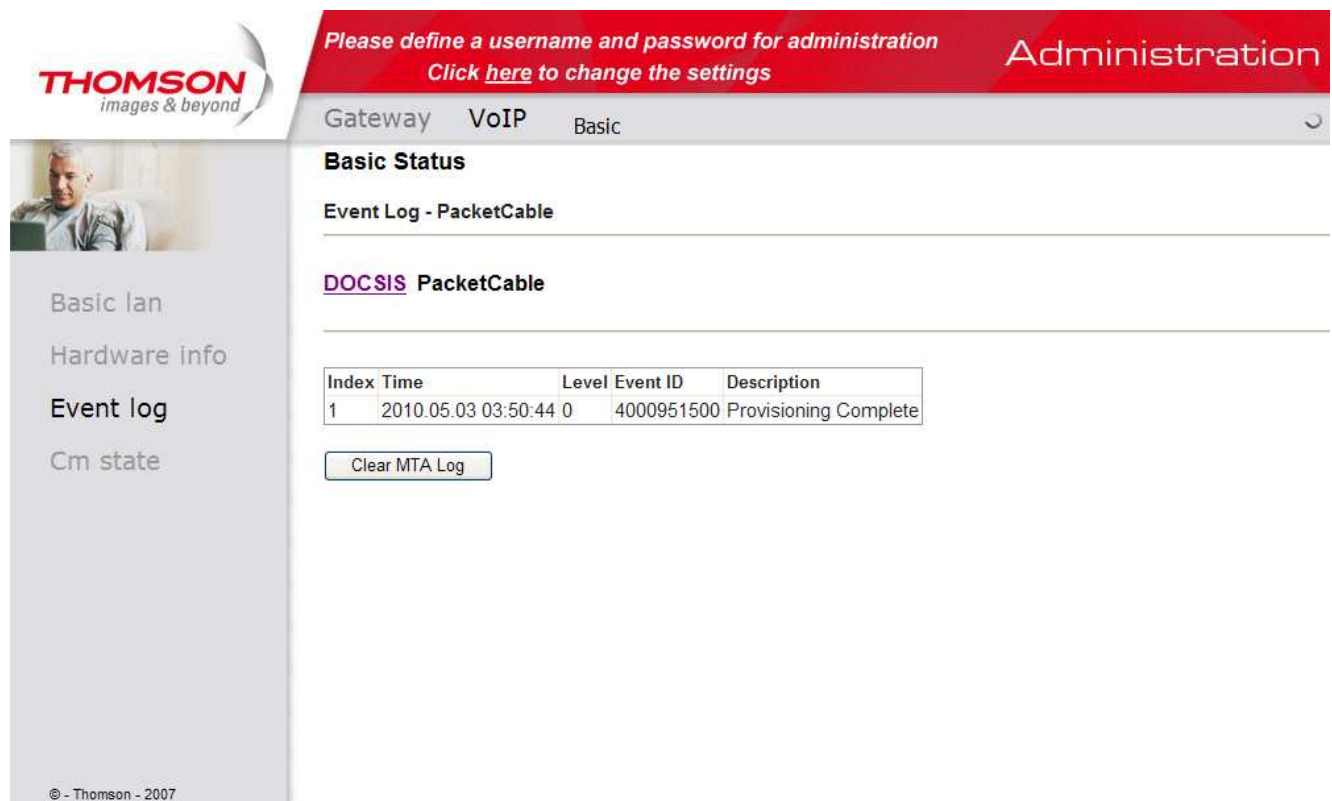
The screenshot shows the Thomson VoIP Basic configuration page. The left sidebar contains navigation links: Basic lan, Hardware info, Event log (selected), and Cm state. The main content area is titled 'Basic Status' and 'Event Log - DOCSIS'. Below this, there is a link for 'DOCSIS PacketCable'. A table displays the event log entries, including Date/Time, Event ID, Event Level, and Description. A 'Clear Log' button is located at the bottom of the table.

Date/Time	Event ID	Event Level	Description
03/30/2010 08.50	82000500	03	Started Unicast Maintenance Ranging - No Response received - T3 time-out;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:15:a7:54:d6:54;CM-QOS=1.1;CM-VER=3.0;
03/29/2010 16.59	68000300	05	DHCP WARNING - Non-critical field invalid in response ;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:15:a7:54:d6:54;CM-QOS=1.1;CM-VER=3.0;
03/29/2010 16.58	66010100	04	Missing BP Configuration Setting TLV Type: 17.9;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:15:a7:54:d6:54;CM-QOS=1.1;CM-VER=3.0;
03/29/2010 16.58	66010100	04	Missing BP Configuration Setting TLV Type: 17.8;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:15:a7:54:d6:54;CM-QOS=1.1;CM-VER=3.0;
01/01/1970 00.00	68000300	05	DHCP WARNING - Non-critical field invalid in response ;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:15:a7:54:d6:54;CM-QOS=1.0;CM-VER=3.0;
01/01/1970 00.00	82000200	03	No Ranging Response received - T3 time-out;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:30:b8:c9:eb:00;CM-QOS=1.0;CM-VER=3.0;
01/01/1970 00.00	82000200	03	No Ranging Response received - T3 time-out;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:15:a7:54:d6:54;CM-QOS=1.0;CM-VER=3.0;
01/01/1970 00.00	84020300	05	MDD message timeout;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:30:b8:c9:eb:00;CM-QOS=1.0;CM-VER=3.0;
01/01/1970 00.00	84020200	05	Lost MDD Timeout;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:30:b8:c9:eb:00;CM-QOS=1.0;CM-VER=3.0;
01/01/1970 00.00	84020200	05	Lost MDD Timeout;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:15:a7:54:d6:54;CM-QOS=1.0;CM-VER=3.0;
01/01/1970 00.00	84020300	05	MDD message timeout;CM-MAC=00:18:9b:3a:c4:87;CMTS-MAC=00:15:a7:54:d6:54;CM-QOS=1.0;CM-VER=3.0;

Clear Log

Fig. 55-1 VoIP\Basic\Event log\DOCSIS

Chapter 2: WEB Configuration



The screenshot displays the Thomson VoIP Basic configuration interface. The top navigation bar is red with the text "Please define a username and password for administration" and "Click [here](#) to change the settings". The "Administration" tab is selected. The left sidebar contains the Thomson logo and a list of menu items: "Basic lan", "Hardware info", "Event log", and "Cm state". The main content area shows the "Basic Status" section with the "Event Log - PacketCable" tab selected. Below this, the "DOCSIS PacketCable" section is visible. A table displays the event log data:

Index	Time	Level	Event ID	Description
1	2010.05.03 03:50:44	0	4000951500	Provisioning Complete

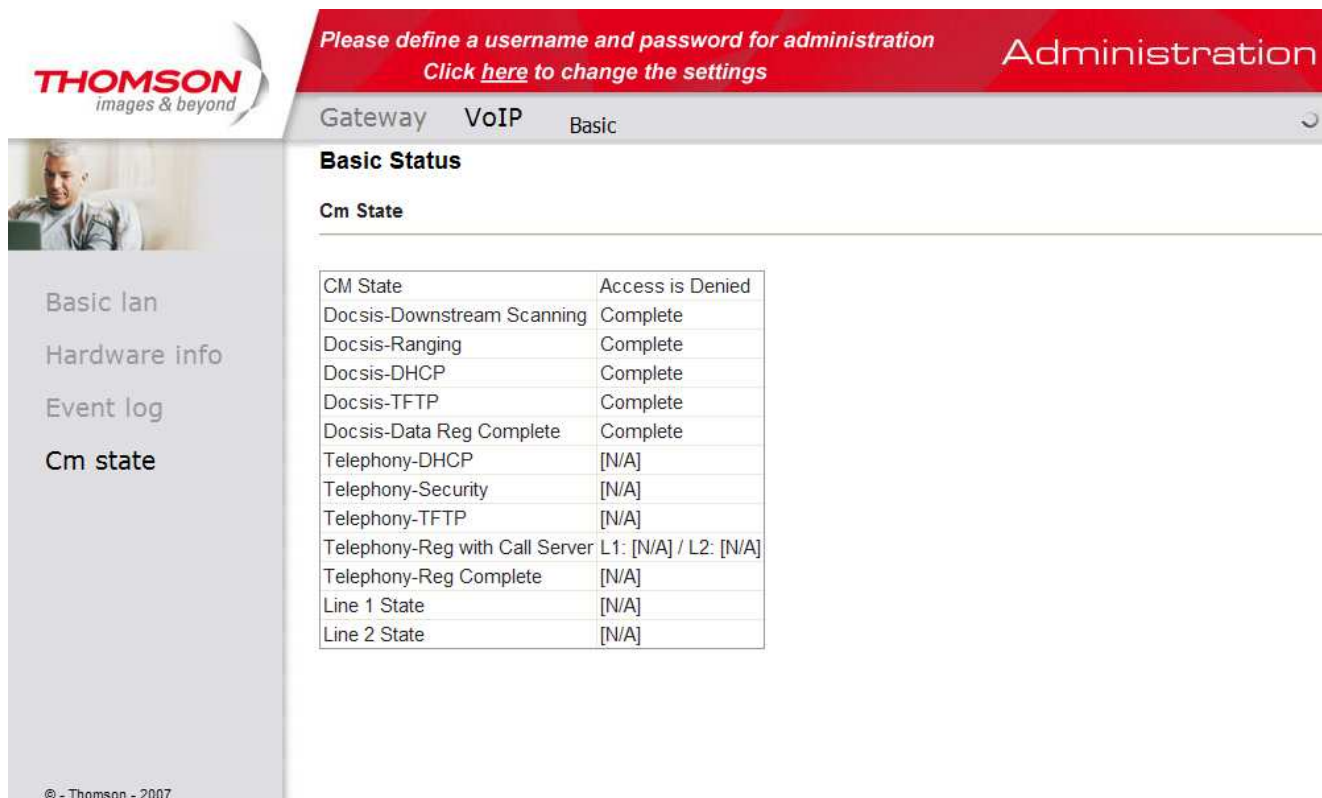
Below the table is a "Clear MTA Log" button. The footer of the page indicates "© - Thomson - 2007".

Fig. 55-2 VoIP\Basic\Event log\PacketCable

Chapter 2: WEB Configuration

4. CM State

This page shows the current state of the cable modem.



The screenshot shows the Thomson Gateway administration interface. The top navigation bar includes 'Gateway', 'VoIP', and 'Basic'. The 'Basic' tab is selected. The main content area is titled 'Basic Status' and contains a section for 'Cm State'. A table displays the current state of various services.

Cm State	
CM State	Access is Denied
Docsis-Downstream Scanning	Complete
Docsis-Ranging	Complete
Docsis-DHCP	Complete
Docsis-TFTP	Complete
Docsis-Data Reg Complete	Complete
Telephony-DHCP	[N/A]
Telephony-Security	[N/A]
Telephony-TFTP	[N/A]
Telephony-Reg with Call Server	L1: [N/A] / L2: [N/A]
Telephony-Reg Complete	[N/A]
Line 1 State	[N/A]
Line 2 State	[N/A]

Fig. 56 VoIP\Basic\Cm state

Chapter 3: Networking

Chapter 3: Networking

Communications

Data communication involves the flow of packets of data from one device to another. These devices include personal computers, Ethernet and USB hubs, cable modems, digital routers and switches, and highly integrated devices that combine functions, like the Wireless Cable Gateway.

The gateway integrates the functionality often found in two separate devices into one. It's both a cable modem and an intelligent wireless gateway networking device that can provide a host of networking features, such as NAT and firewall. Figure 2 illustrates this concept, with the cable modem (CM) functionality on the left, and networking functionality on the right. In this figure, the numbered arrows represent communication based on source and destination, as follows:

Type of Communication

1. Communication between the Internet and your PCs

Example: The packets created by your request for a page stored at a web site, and the contents of that page sent to your PC.

2. Communication between your cable company and the cable modem side

Example: When your cable modem starts up, it must initialize with the cable company, which requires the cable company to communicate directly with the cable modem itself.

3. Communication between your PCs and the networking side

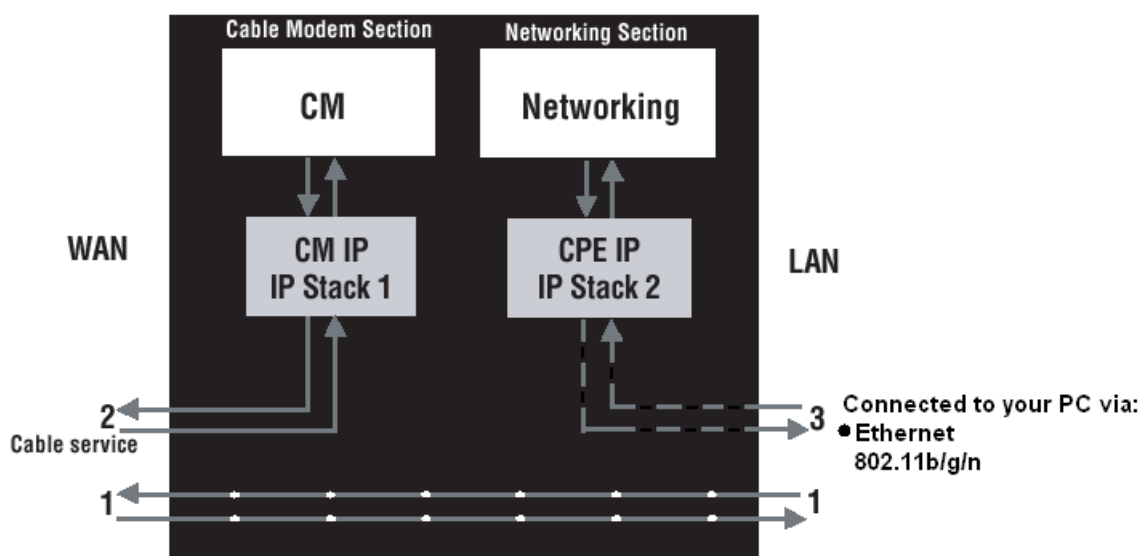


Fig.57 Communication between your PCs and the network side

Example: The Wireless Cable Gateway offers a number of built-in web pages which you can use to configure its networking side; when you communicate with the networking side, your communication is following this path.

Chapter 3: Networking

Each packet on the Internet addressed to a PC in your home travels from the Internet downstream on the cable company's system to the WAN side of your Wireless Cable Gateway. There it enters the Cable Modem section, which inspects the packet, and, based on the results, proceeds to either forward or block the packet from proceeding on to the Networking section. Similarly, the Networking section then decides whether to forward or block the packet from proceeding on to your PC. Communication from your home device to an Internet device works similarly, but in reverse, with the packet traveling upstream on the cable system.

Cable Modem (CM) Section

The cable modem (or CM) section of your gateway uses EURO-DOCSIS Standard cable modem technology. EURO-DOCSIS specifies that TCP/IP over Ethernet style data communication be used between the WAN interface of your cable modem and your cable company.

A EURO-DOCSIS modem, when connected to a Cable System equipped to support such modems, performs a fully automated initialization process that requires no user intervention. Part of this initialization configures the cable modem with a CM IP (Cable Modem Internet Protocol) address, as shown in Figure 3, so the cable company can communicate directly with the CM itself.

Networking Section

The Networking section of your gateway also uses TCP/IP (Transmission Control Protocol/ Internet Protocol) for the PCs you connected on the LAN side. TCP/IP is a networking protocol that provides communication across interconnected networks, between computers with diverse hardware architectures and various operating systems.

TCP/IP requires that each communicating device be configured with one or more TCP/IP stacks, as illustrated by Figure 4. On a PC, you often use software that came with the PC or its network interface (if you purchased a network interface card separately) to perform this configuration. To communicate with the Internet, the stack must also be assigned an IP (Internet Protocol) address. 192.168.100.1 is an example of an IP address. A TCP/IP stack can be configured to get this IP address by various means, including a DHCP server, by you directly entering it, or sometimes by a PC generating one of its own.

Ethernet requires that each TCP/IP stack on the Wireless Cable Gateway also have associated with it an Ethernet MAC (Media Access Control) address. MAC addresses are permanently fixed into network devices at the time of their manufacture. 00:90:64:12:B1:91 is an example of a MAC address.

Data packets enter and exit a device through one of its network interfaces. The gateway offers Ethernet and 802.11b/g wireless network interfaces on the LAN side and the EURO-DOCSIS network interface on the WAN side.

When a packet enters a network interface, it is offered to all the TCP/IP stacks associated with the device side from which it entered. But only one stack can accept it — a stack whose configured Ethernet address matches the Ethernet destination address inside the packet. Furthermore, at a packet's final destination, its destination IP address must also match the IP address of the stack.

Each packet that enters a device contains source MAC and IP addresses telling where it came from, and destination MAC and IP addresses telling where it is going to. In addition, the packet contains all or part of a message destined for some application that is running on the destination device. IRC used

Chapter 3: Networking

in an Internet instant messaging program, HTTP used by a web browser, and FTP used by a file transfer program are all examples of applications. Inside the packet, these applications are designated by their port number. Port 80, the standard HTTP port, is an example of a port number.

The Networking section of the router performs many elegant functions by recognizing different packet types based upon their contents, such as source and destination MAC address, IP address, and ports.

Three Networking Modes

Your gateway can be configured to provide connectivity between your cable company and your home LAN in any one of three Networking Modes: CM, RG, and CH. This mode setting is under the control of your cable company, who can select the mode to match the level of home networking support for which you have subscribed. All units ship from the factory set for the RG mode, but a configuration file which the cable company sends the cable modem section during its initialization can change it.

Cable Modem (CM) Mode

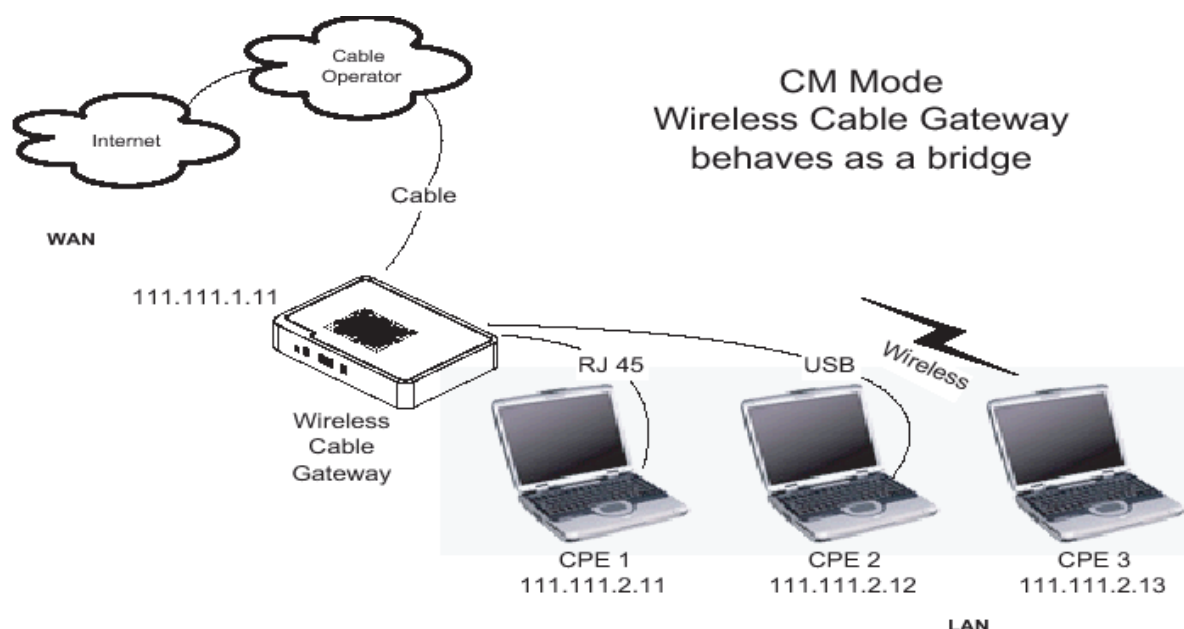


Fig. 58 Cable Modem Mode

Chapter 3: Networking

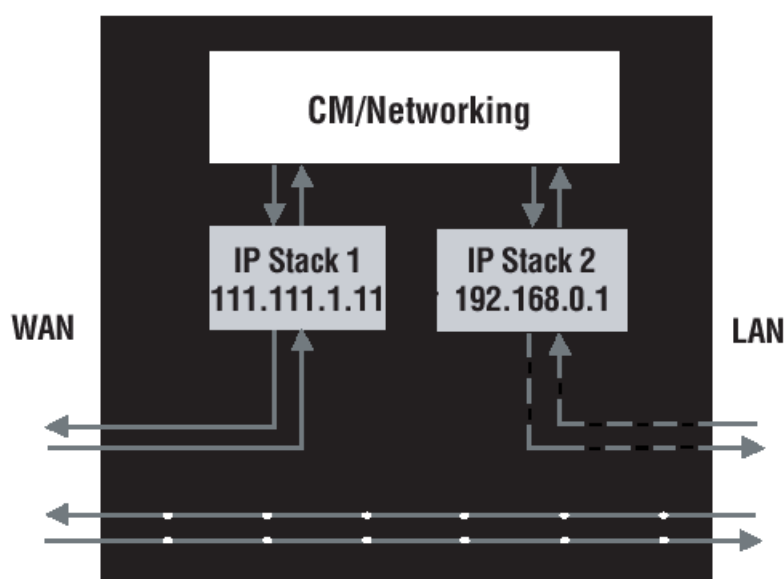


Fig. 59 Two IP stacks are activated in cable modem mode

CM (Cable Modem) Mode provides basic home networking. In this mode, two IP stacks are active:

- IP Stack 1 - for use by the cable company to communicate with the cable modem section only. This stack receives its IP address from the cable company during CM initialization. It uses the MAC address printed on the label attached to the Wireless Cable gateway.
- IP Stack 2 - for use by you, the end user, to communicate with the cable modem and Networking sections, to access the internal web page diagnostics and configuration. This stack uses a fixed IP address: 192.168.100.1. It uses a MAC address of MAC label + 1 (the MAC label is found on the bottom of the unit). E.g., if the MAC address is 00:90:64:12:B1:91, this MAC address would be 00:90:64:12:B1:92.

With CM Mode, your cable company must provide one IP address for the CM section, plus one for each PC you connect from their pool of available addresses. Your cable company may have you or your installer manually enter these assigned addresses into your PC, or use a DHCP Server to communicate them to your PCs, or use a method that involves you entering host names into your PCs.

Note that in CM Mode, packets passing to the Internet to/from your PCs do not travel through any of the IP stacks; instead they are directly bridged between the WAN and LAN sides.

Chapter 3: Networking

Residential Gateway (RG) Mode

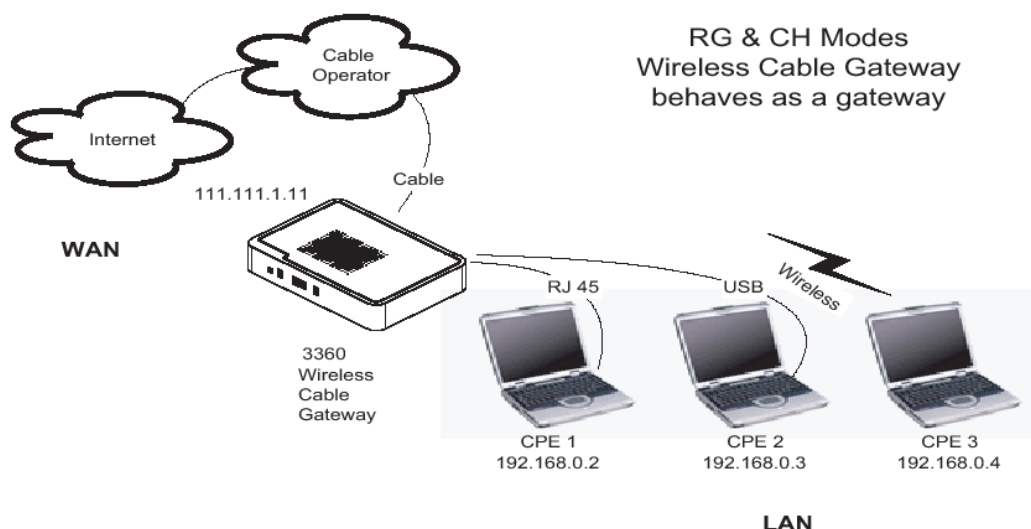


Fig. 60 Residential Gateway Mode

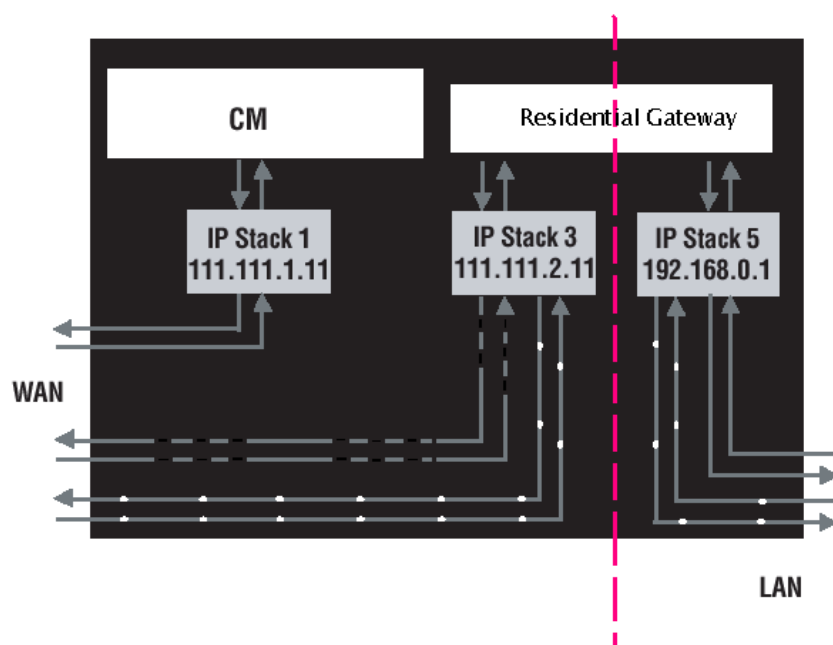


Fig. 61 Three IP stacks are activated in Residential mode

RG (Residential Gateway) Mode provides basic home networking plus NAT (Network Address Translation). In this mode, three IP stacks are active:

- IP Stack 1 - for use by the cable company to communicate with the Cable Modem section only. This stack receives its IP address from the cable company during CM initialization. It uses the MAC address printed on the label attached to the Wireless Cable Gateway.
- IP Stack 3 - for use by you to remotely (i.e. from somewhere on the WAN side, such as at your remote workplace) communicate with the Cable Modem and Networking sections, to remotely access the internal web page diagnostics and configuration. This stack is also used by your cable

Chapter 3: Networking

company to deliver packets between the Internet and the gateway's networking section so they can be routed to/from your PCs. This stack requires an IP address assigned by the cable company from their pool of available addresses. Your cable company may have you or your installer manually enter assigned addresses into your gateway, or use a DHCP Server to communicate them, or use a method that involves you entering host names. This stack uses a MAC address of MAC label + 2 (the MAC label is found on the bottom of the unit). E.g., if the MAC address is 00:90:64:12:B1:91, this MAC address would be 00:90:64:12:B1:93.

- IP Stack 5 - for use by you to locally (i.e. from somewhere on the LAN side in your home) communicate with the Cable Modem and Networking sections, to access the internal web page diagnostics and configuration. This stack is also used by the gateway's networking section to route packets between the gateway's Networking section and your PCs. This stack uses a fixed IP address: 192.168.0.1. It uses a MAC address of MAC label + 4 (the MAC label is found on the bottom of the unit). E.g., if the MAC address is 00:90:64:12:B1:91, this MAC address would be 00:90:64:12:B1:95.

With RG Mode, your cable company must provide one IP address for the CM section, plus one for the Networking section, from their pool of available addresses. With RG Mode, each PC you connect gets an IP address from a DHCP Server that is part of the Networking section of the gateway.

Chapter 4: Additional Information

Chapter 4: Additional Information

Frequently Asked Questions

Q. What if I don't subscribe to cable TV?

A. If cable TV is available in your area, data and voice service may be made available with or without cable TV service. Contact your local cable company for complete information on cable services, including high-speed internet access.

Q. How do I get the system installed?

A. Professional installation from your cable provider is strongly recommended. They will ensure proper cable connection to the modem and your computer. However, your retailer may have offered a self installation kit, including the necessary software to communicate with your cable ISP.

Q. My modem is connected to the power sector but does not work

A. Check the ON/OFF button on the rear panel of your modem. It should be set to "1".

Q. Once my Wireless Voice Gateway is connected, how do I get access to the Internet?

A. Your local cable company provides your internet service*, offering a wide range of services including email, chat, and news and information services, and a connection to the World Wide Web.

Q. It seems that the wireless network is not working

A. Check the WiFi LED on the front panel. If it is no lighted, press on the WPS/Wifi button shortly, less than 1 second, on the side of the modem, and then check again the WiFi LED. If it is lighted, then the WiFi is enabled.

Q. Can I watch TV, surf the Internet, and talk to my friends through the Wireless Voice Gateway at the same time?

A. Absolutely!

Q. What do you mean by "Broadband?"

A. Simply put, it means you'll be getting information through a "bigger pipe," with more bandwidth, than a standard phone line can offer. A wider, "broader" band means more information, more quickly.

Q. What is Euro-DOCSIS and what does it mean?

A. "Data over Cable Service Interface Specifications" is the industry standard that most cable companies

Chapter 4: Additional Information

are adopting as they upgrade their systems. Should you ever decide to move, the Wireless Voice Gateway will work with all upgraded cable systems that are Euro-DOCSIS-compliant.

Q. What is Euro-PacketCable and what does it mean?

A. Euro-PacketCable is the industry standard for telephony services that most cable companies are adopting as they upgrade their systems. Should you ever decide to move, the Wireless Voice Gateway will work with all upgraded cable systems that are Euro-PacketCable compliant.

Q. What is Xpress Technology and what does it mean?

A. It is one of the popular performance-enhancing WiFi technologies, designed to improve wireless network efficiency and boost throughput. It is more efficient in mixed environments, and it can work with 802.11a/b/g networks. When Xpress is turned on, aggregate throughput (the sum of the individual throughput speeds of each client on the network) can improve by **up to** 27% in 802.11g-only networks, and **up to** 75% in mixed networks comprised of 802.11g and 802.11b standard equipment. The technology achieves higher throughput by re-packaging data, reducing the number of overhead control packets, so that more useful data can be sent during a given amount of time.

* Monthly subscription fee applies.

** Additional equipment required. Contact your cable company and ISP for any restrictions or additional fees.

Chapter 4: Additional Information

General Troubleshooting

You can correct most problems you have with your product by consulting the troubleshooting list that follows.

I can't access the internet.

- Check all of the connections to your Wireless Voice Gateway.
- Your Ethernet card may not be working. Check each product's documentation for more information.
- The Network Properties of your operating system may not be installed correctly or the settings may be incorrect. Check with your ISP or cable company.

I can't get the modem to establish an Ethernet connection.

- Even new computers don't always have Ethernet capabilities – be sure to verify that your computer has a properly installed Ethernet card and the driver software to support it.
- Check to see that you are using the right type of Ethernet cable.

The modem won't register a cable connection.

- If the modem is in Initialization Mode, the INTERNET light will be flashing. Call your Cable Company if it has not completed this 5-step process within 30 minutes, and note which step it is getting stuck on.
- The modem should work with a standard RG-6 coaxial cable, but if you're using a cable other than the one your Cable Company recommends, or if the terminal connections are loose, it may not work. Check with your Cable Company to determine whether you're using the correct cable.
- If you subscribe to video service over cable, the cable signal may not be reaching the modem. Confirm that good quality cable television pictures are available to the coaxial connector you are using by connecting a television to it. If your cable outlet is "dead", call your Cable Company.
- Verify that the Cable Modem service is Euro-DOCSIS compliant and Euro-PacketCable compliant by calling your cable provider.

I don't hear a dial tone when I use a telephone.

- Telephone service is not activated. If the rightmost light on the Wireless Voice Gateway stays on while others flash, check with your TSP or cable company.
- If the Wireless Voice Gateway is connected to existing house telephone wiring, make sure that

Chapter 4: Additional Information

another telephone service is not connected. The other service can normally be disconnected at the Network Interface Device located on the outside of the house.

- If using the second line on a two-line telephone, use a 2-line to 1-line adapter cable.

For more Usage and Troubleshooting Tips use the web site links provided on the CD-ROM:

<http://www.Technicolor.net/GlobalEnglish/Deliver/Cable/cable-modems-routers-gateways/Pages/default.aspx>

Service Information

If you purchased or leased your Wireless Voice Gateway directly from your cable company, then warranty service for the Digital Cable Modem may be provided through your cable provider or its authorized representative. For information on 1) Ordering Service, 2) Obtaining Customer Support, or 3) Additional

Chapter 4: Additional Information

Service Information, please contact your cable company. If you purchased your Wireless Voice Gateway from a retailer, see the enclosed warranty card.

Glossary

10/100/1000 BaseT – Unshielded, twisted pair cable with an RJ-45 connector, used with Ethernet LAN (Local Area Network). “10/100/1000” indicates speed (10/100/1000 BaseT), “Base” refers to baseband technology, and “T” means twisted pair cable.

Authentication - The process of verifying the identity of an entity on a network.

Chapter 4: Additional Information

DHCP (Dynamic Host Control Protocol) – A protocol which allows a server to dynamically assign IP addresses to workstations on the fly.

Ethernet adapters – A plug-in circuit board installed in an expansion slot of a personal computer. The Ethernet card (sometimes called a Network Interface Card , network adapter or NIC) takes parallel data from the computer, converts it to serial data, puts it into a packet format, and sends it over the 10/100/1000 BaseT LAN cable.

Euro-DOCSIS (Data Over Cable Service Interface Specifications) – A project with the objective of developing a set of necessary specifications and operations support interface specifications for Cable Modems and associated equipment.

F Connector – A type of coaxial connector, labeled CABLE IN on the rear of the Wireless Voice Gateway that connects the modem to the cable system.

HTTP (HyperText Transfer Protocol) – Invisible to the user, HTTP is used by servers and clients to communicate and display information on a client browser.

Hub – A device used to connect multiple computers to the Wireless Voice Gateway.

IP Address – A unique, 32-bit address assigned to every device in a network. An IP (Internet Protocol) address has two parts: a network address and a host address. This modem receives a new IP address from your cable operator via DHCP each time it goes through Initialization Mode.

Key exchange - The swapping of mathematical values between entities on a network in order to allow encrypted communication between them.

MAC Address – The permanent “identity” for a device programmed into the Media Access Control layer in the network architecture during the modem’s manufacture.

NID - Network Interface Device, the interconnection between the internal house telephone wiring and a conventional telephone service provider’s equipment. These wiring connections are normally housed in a small plastic box located on an outer wall of the house. It is the legal demarcation between the subscriber’s property and the service provider’s property.

Euro-PacketCable – A project with the objective of developing a set of necessary telephony specifications and operations support interface specifications for Wireless Voice Gateways and associated equipment used over the Euro-DOCSIS based cable network.

PSTN (Public Switched Telephone Network) – The worldwide voice telephone network which provides dial tone, ringing, full-duplex voice band audio and optional services using standard telephones.

Provisioning - The process of enabling the Media Terminal Adapter (MTA) to register and provide

Chapter 4: Additional Information

services over the network.

TCP/IP (Transmission Control Protocol/Internet Protocol) – A networking protocol that provides communication across interconnected networks, between computers with diverse hardware architectures and various operating systems.

TFTP - Trivial File Transfer Protocol, the system by which the Media Terminal Adapter's configuration data file is downloaded.

TSP - Telephony Service Provider, an organization that provides telephone services such as dial tone, local service, long distance, billing and records, and maintenance.

Universal Serial Bus (USB) – USB is a “plug-and-play” interface between a computer and add-on devices, such as a Wireless Voice Gateway.

Xpress Technology - One of the popular performance-enhancing WiFi technologies, designed to improve wireless network efficiency and boost throughput. It is more efficient in mixed environments, and it can work with 802.11a/b/g networks.

Please do not send any products to the Indianapolis address listed in this manual or on the carton. This will only add delays in service for your product.

Thomson Inc.

101 W. 103rd St., INH700

Indianapolis, IN 46290

USA

For more information

Technicolor | 1 rue Jeanned'Arc | 92443 Issy les Moulineaux | France
Tel. : 33 (0) 1 41 86 50 00 | Fax : 33 (0) 1 41 86 56 59 | www.thomson-broadband.com

© 2007 Thomson Inc. - Trademark(s) * Registered\ - Marca(s) Registrada(s)\
Photos and features subject to change without notice.
Illustration of product finish may vary from actual color.

THOMSON